ホ ー ル

群　　論

(下)

榎本彦衛
坂内英一　訳

数学叢書
13

吉岡書店

THE THEORY OF GROUPS

by

Marshall Hall, Jr.

目　　次

（下　巻）

1), 2) ……は訳者注　　*), **) は原著者注

第11章　基底交換子

11.1. 集　中　過　程

記号の集合 $x_1, \cdots, x_n$ から作られた形式的な語（formal word または formal string）について考えることが以下の目標である．いま，**形式的交換子**（formal commutator）$c_i (i=1, 2, \cdots)$ とその重さ（weight）$\omega(c_i)$ を次の 2 つの規則によって定義する．

1）$x_i (i=1, \cdots, r)$ はいずれも交換子であると定め，その重さを 1 と定める．すなわち $\omega(x_i)=1$

2）c_i と c_j が交換子ならば，$c_k=(c_i, c_j)$ も交換子であると定め，その重さを $\omega(c_k)=\omega(c_i)+\omega(c_j)$ で定める．

この定義から分かるように，与えられた重さを持つ交換子は有限個しかないことに注意しなければならない．次に，添字をつけることによって交換子に順序を入れよう．まず，$c_i=x_i (i=1, \cdots, r)$ と置く．重さ 1 の交換子はこれでつきる．次に，重さ 2 の交換子全部に適当に順番をつけてならべ，それらを c_{r+1}, $c_{r+2}, \cdots$ と置く．次に重さ 3 の交換子全部を適当に順番をつけてならべる，……，という具合にして，交換子全体に（線型な）順序を入れる。

記号の集合として交換子全体をとったときにできた語 $c_{i_1} c_{i_2} \cdots c_{i_m}$ が**集中形**（collected form）であるとは，$i_1 \leqq i_2 \leqq \cdots \leqq i_m$ であることをいう．すなわち，交換子 $c_{i_1}, \cdots, c_{i_m}$ 達が上で定めた順序に従っていることをいう．さて，交換子からなる任意の語

$$c_{i_1} \cdots c_{i_m} c_{i_{m+1}} \cdots c_{i_n} \tag{11.1.1}$$

に対して，$i_1 \leqq \cdots \leqq i_m$, $i_m \leqq i_j (j=m+1, \cdots, n)$ であり，かつ適当な $j \geqq m+1$ が存在して，$i_{m+1} > i_j$ であるとき，$c_{i_1} \cdots c_{i_m}$ を集中部分 $c_{i_{m+1}} \cdots c_{i_n}$ を非集中部分とよぶことにする．**集中部分**，**非集中部分**は空であってもかまわない．

次に，交換子からなる語に対して**集中過程** (collecting process) とよばれる演算を定義する．すなわち，非集中部分に属する交換子のうち一番順序の若いものを c_u とする．非集中部分に属する交換子で c_u に等しいもののうち一番左側にある交換子を c_{i_j} とする．このとき，$c_{i_1}\cdots c_{i_m}\cdots c_{i_{j-1}}c_{i_j}\cdots c_{i_n}$ を $c_{i_1}\cdots c_{i_m}\cdots c_{i_j}c_{i_{j-1}}(c_{i_{j-1}}, c_{i_j})\cdots c_{i_n}$ に置き換える写像を集中過程とよぶ．この演算によって，c_{i_j} は1つ左に動き，そのかわりに c_{i_j} より重さの大きい交換子 $(c_{i_{j-1}}, c_{i_j})$ が新しく差し込まれる．したがってこの過程をつづけても c_{i_j} は依然として非集中部分の中で一番順序が若い交換子である．そこで何回かこの集中過程を繰り返すことによって c_{i_j} は左から $(m+1)$ 番目の場所に移され，したがって集中部分にくみこまれてしまう．ところでこの過程は，各演算ごとに新しい交換子が導入されるので，この演算はいつまでたっても終わらないかもしれないということに注意しなければならない．

いま，$x_1, \cdots, x_r$ を群 F の生成元とする．我々に興味があるのは特に F がこれらで生成された自由群の場合である．このとき，交換子 $(u, v)=u^{-1}v^{-1}uv$ だから，F の元として，

(11.1.2) $$c_{i_{j-1}}c_{i_j}=c_{i_j}c_{i_{j-1}}(c_{i_{j-1}}, c_{i_j})$$

であるから，集中過程は群 F の元それ自身を変えない．ところで，上で定義した集中過程は F の元全体に対しては定義されていない．すなわち，F の元で生成元の逆元を用いないで表わされる語（**正の語** (positive word) とよぶ）に対してのみ定義されている．後でこの欠点を改めよう．

いま，正の元に集中過程をほどこしたとき，交換子すべてがその中に現われるわけではない．実際，(x_2, x_1) は現われるが，(x_1, x_2) は，x_1 が x_2 の先に集中過程の適用を受けるから，現われることはない．そこで，正の語に集中過程をほどこしたときに現われる交換子を**基底交換子** (basic commutator) とよぶことにする．次に，この定義をはっきりさせるために，$x_1, \cdots, x_r$ から生成された自由群に対して，基底交換子の形式的定義を与える．

基底交換子の定義：

1)　$c_i=x_i$ ($i=1, \cdots, r$) は基底交換子であり，その重さを1と定義する．$\omega(c_i)=1$ で表わす．

2)　重さ $n-1$ 以下の基底交換子がすべて定まったとき，重さnの基底交換子とは次の2条件を満たす c_i, c_j からなる交換子 (c_i, c_j) である．

(a)　c_i, c_j は基底交換子で $\omega(c_i)+\omega(c_j)=n$

(b)　$c_i>c_j$ また，$c_i=(c_s, c_t)$ ならば，$c_j\geqq c_t$

3)　交換子の場合と同様に基底交換子全体の集合に線型順序を入れる．すなわち，重さの小さいものは重さの大きいものの前になるようにし，同じ重さのものの間には適当に順序をつけて固定する．そこで，このようにして並べた順に添字をつける．

交換子からなる正の語に集中過程を適用したとき，基底交換子のみが現われる．なぜならば

(11.1.3)
$$c_uc_v=c_vc_u(c_u, c_v)$$

と置き換える際には，集中過程を c_u よりも先に c_v に対して適用させるから，$c_u>c_v$ であり，またもし $c_u=(c_s, c_t)$ ならば，c_v より先に c_t に対して適用させるから $c_v\geqq c_t$ でなければならないからである．

さて話は変って，$\Gamma_{k+1}(F)(=F_{k+1}$ と書く）を群Fの降中心鎖 (lower central series) の $(k+1)$ 番目の要素としたとき，Fの任意の元fは

(11.1.4)
$$f=c_1^{e_1}c_2^{e_2}\cdots c_t^{e_t} \bmod F_{k+1}$$

と書けることを示す．ここで，$c_1, \cdots, c_t$ は重さがk以下の基底交換子全体を順序に従ってならべたものである．集中過程において，

(11.1.5)
$$vu=uv(v, u)$$

を得る，ここで$u, v, (v, u)$ はいずれも基底交換子である．次に $vu^{-1}, v^{-1}u^{-1}$, $v^{-1}u$ などの型で現われている u, u^{-1} に集中過程の演算を作用させる．いま，$vu^{-1}=u^{-1}v(v, u^{-1})$ であるから (10.2.13) により

(11.1.6)
$$1=(v, uu^{-1})=(v, u^{-1})(v, u)(v, u, u^{-1})$$

を得る．したがって $(v, u^{-1})=(v, u, u^{-1})^{-1}(v, u)^{-1}$ である．同様に，$(v, u, u^{-1})=(v, u, u, u^{-1})^{-1}(v, u, u)^{-1}$ である．次に $v_0=v,\ v_{t+1}=(v_t, u)$ と置く．この

とき，

(11.1.7)
$$(v, u^{-1})=(v_1, u^{-1})^{-1}v_1^{-1}$$
$$=v_2(v_3, u^{-1})v_1^{-1}$$
$$=v_2v_4\cdots v_5^{-1}v_3^{-1}v_1^{-1} \pmod{F_{k+1}}$$

を得る，このとき，もし $v_1=(v, u)$ が基底交換子であれば，$v_2, v_3, \cdots$ も基底交換子である．いま，modulo F_{k+1} で考えているから，(v_s, u^{-1}) の重さが $k+1$ 以上になるような十分大きな s については (v_s, u^{-1}) を無視することができる．したがって

(11.1.8)
$$vu^{-1}=u^{-1}vv_2v_4\cdots v_5^{-1}v_3^{-1}v_1^{-1} \pmod{F_{k+1}}$$

である。同様に，

(11.1.9)
$$v^{-1}u=uv^{-1}(v^{-1}, u)$$

である．

一方，$v^{-1}u^{-1}=u^{-1}(uvu^{-1})^{-1}$ であり，(11.1.8) から

(11.1.10)
$$uvu^{-1}=vv_2v_4\cdots v_5^{-1}v_3^{-1}v_1^{-1} \pmod{F_{k+1}}$$

を得る．したがって

(11.1.11)
$$v^{-1}u^{-1}=u^{-1}v_1v_3v_5\cdots v_4^{-1}v_2^{-1}v^{-1} \pmod{F_{k+1}}$$

である．そこで (11.1.5, -8, -9, -11) をなんどか繰り返せば，任意の元 f に対して，(11.1.4) における基底交換子を用いた表現が得られる．

もし F が $x_1, x_2, \cdots, x_r$ から生成された自由群であれば，(11.1.4) における表現は一意的に定まる． このことは次の §11.2 で示される．特に重さ k の基底交換子達は，自由アーベル群 F_k/F_{k+1} の自由基底を作る．基底交換子という名称はこのことに由来している．

11.2. Witt の公式と基底定理

$c_1, c_2, \cdots$ を生成元 $x_1, \cdots, x_n$ から作られた基底交換子の列とする．(先に定めた順序に従ってならんでいるものとする。) いま，基底交換子の積，

(11.2.1)
$$c_{i_1}c_{i_2}\cdots c_{i_n}$$

が集中形であるとき，すなわち $i_1 \leqq i_2 \leqq \cdots \leqq i_n$ のとき，この積を基本積とよぶ

ことにする．次に，交換子 a_i 達の積 $p=a_1\cdots a_n$ に対して，その重さ $\omega(p)$ を $\omega(p)=\omega(a_1)+\cdots+\omega(a_n)$ で定義する．ところで，集中過程は積の重さを変えてしまう．そこで，次のような括弧過程 (bracketing process) という積の重さを変えない演算を考える．すなわち，$u, v, (u, v)$ が基底交換子であるとき，uv を (u, v) で置き換えるのである．なお，集中過程のときは，uv を $vu(u, v)$ で置き換えたことに注意しよう．

定理 11.2.1. 生成元 $x_1, \cdots, x_r$ から作られた重さ n の基本積の個数は r^n である．

証：各 $k=1, 2\cdots$ に対して，$P_k=P_k^{(n)}$ を，基底交換子の積で重さが n で $c_1^{e_1}c_2^{e_2}\cdots c_k^{e_k}c_{i_1}\cdots c_{i_s}$，(ここで，$e_i\geqq 0, i_1>k, i_2, \cdots, i_s\geqq k$ かつ各交換子 $c_{i_j}(j=1, \cdots, s)$ は，$c_{i_j}=(c_u, c_v)$ ならば，c_v が c_k に先行している)，と書かれるもの全体からなる集合と定義する．したがって，P_k は c_{k-1} まではすでに集中過程の適用を受けて，c_k に関してはまだであるような，基底交換子の積達からできている集合である．P_k に含まれる元の個数を $|P_k|$ で表わす．明らかに，P_1 は生成元の n 個の積全体からなり，$|P_1|=r^n$ である．次に，集合 P_k と P_{k+1} の間に 1 対 1 の対応をつける．いま，$c_1^{e_1}\cdots c_k^{e_k}c_{i_1}\cdots c_{i_s}$ が P の元であるとする．したがって，$c_k<c_{i_1}$ であり，もし c_{i_j} のうちに c_k がいくつか引きつづいてあらわれれば，その直前の元 c_y に対しては $y>k$ である．いま，次のような各々の語（積）

$$c_yc_k\cdots c_kc_w \qquad y>k, w>k$$

に対して，$(\cdots((c_y, c_k), c_k), \cdots c_k)c_w$ と括弧をつける．いま，$c_y=(c_u, c_v)$，ならば $k>v$ だから，$(\cdots((c_y, c_k), c_k), \cdots c_k)$ は基底交換子であり，c_k よりも順番が遅い．したがって，この括弧づけを $c_1^{e_1}\cdots c_k^{e_k}c_{i_1}\cdots c_{i_s}$ にほどこすことにより，P_{k+1} の元が一意的に定まる．逆に，P_{k+1} の任意の元に対しては，c_k をうしろに含んでいるような括弧をすべて取り除くことにより，P_k の元が一意的に定まる．したがって $|P_k|=|P_{k+1}|$ であり，各 k に対して，$|P_k|=|P_1|=r^n$ である．ところで k を十分大きくとれば，P_k は重さ n の基本積だけから成っ

ている．したがって定理の証明は完成した．

この定理11.2.1を用いることにより，重さnの基底交換子の個数，さらに，各生成元に関する重さが定められた基底交換子の個数を求めることができる．ここで，各生成元x_iに関する重さ$\omega_i(c)(i=1, \cdots, r)$とは，$\omega_i(x_i)=1, \omega_i(x_j)=0(i\neq j)$, $\omega_i[(c_u, c_v)]=\omega_i(c_u)+\omega_i(c_v)$により帰納的に定めたものである．いま，$M_r(n)$を$r$個の生成元$x_1, x_2, \cdots x_r$から作られる重さ$n$の基底交換子の個数，$M(n_1, n_2, \cdots n_r)$を$\omega_i(c)=n_i(i=1, \cdots, r,\ n=n_1+\cdots+n_r)$なる基底交換子$c$の個数とする．このとき，次の定理が成り立つ．

定理 11.2.2.（Witt の定理）

(11.2.3) $$M_r(n)=\frac{1}{n}\sum_{d|n}\mu(d)r^{n/d}$$

(11.2.4) $$M(n_1, n_2, \cdots, n_r)=\frac{1}{n}\sum_{d|n_1, \cdots, n_r}\mu(d)\left(\frac{n}{d}\right)!\Big/\left(\frac{n_1}{d}\right)!\cdots\left(\frac{n_r}{d}\right)!$$

ここで$\mu(m)$は Möbius 関数を表わす．すなわち，μは正整数に対してのみ定義され，$\mu(1)=+1$，かつ$m=p_1^{e_1}\cdots p_s^{e_s}(p_1, \cdots, p_s$は相異なる素数)に対してはある$i$に対して$e_i>1$が成り立つとき，$\mu(m)=0$，そうでないとき$\mu(m)=\mu(p_1\cdots p_s)=(-1)^s$である．

証：定理11.2.1により，重さnの基本積の個数はr^nである．したがって，変数zに関する形式的巾級数としての恒等式

(11.2.5) $$\frac{1}{1-rz}=\prod_{n=1}^{\infty}(1-z^n)^{-M_r(n)}$$

が導かれる．一方，括弧過程はすべての重さ$\omega_i(i=1, \cdots, r)$を不変に保つ．したがって，$\omega_i(W)=n_i(i=1, \cdots, r)$を満たす語$W$の個数は多項係数

$$\frac{n!}{n_1!\cdots n_r!}$$

で与えられる．したがって，変数$z_1, \cdots, z_r$に関しての形式的巾級数としての恒等式

(11.2.6) $$\frac{1}{1-z_1-\cdots-z_r}=\prod_{n_1, \cdots, n_r=0}^{\infty}(1-z_1^{n_1}\cdots z_r^{n_r})^{-M(n_1, \cdots, n_r)}$$

が導かれる．Witt [2] は，これらの恒等式に対して，まず対数をとり，次に

Möbius の反転公式を用いることにより，式 (11.2.3) (11.2.4) を証明した．ここでは，定理 11.2.1 を証明したのと同様の方法を用いてこの定理を証明する．これは Meier-Wunderli [1] における証明を改良したものである．

語 $a_1a_2\cdots a_n$, $a_2\cdots a_na_1$, $\cdots$, $a_na_1\cdots a_{n-1}$ をすべて同一視したとき，語 $a_1a_2\cdots a_n$ を巡回語であるということにする．いま，巡回語が d 個の文字からなる語を何回か繰り返すことによりできているとき，d を周期とよぶ．このときこの d 個の文字からなる語を巡回部分とよぶことにする．各巡回語に対して，最小の周期 d が一意的に定まる．またこのとき長さ d の巡回語が一意的に定まる．

補題 11.2.1. 重さ n の基底交換子全体の集合と，長さ n，最小の周期 n の巡回語全体の集合との間に 1 対 1 の対応がつく．この対応は，巡回語に適当に括弧をつけることにより得られる．

証：$a_1a_2\cdots a_n$ を長さ n の巡回語とする．いま，次の条件（1），（2）を満たす重さ n の巡回語全体からなる集合を $C_k{}^n=C_k$ で表わす．

1)　$c_{i_1}c_{i_2}\cdots c_{i_s}$（各 c_{i_j} は基底交換子）と表わされ，各 $c_{i_j}=(c_u, c_v)$ に対して $v<k$ である．

2)　次の i) または ii) の少なくとも一方が成り立つ．i) $i_1=i_2=\cdots=i_s$ ($s=1$ の場合も含む)，ii) $i_1, \cdots, i_s\geqq k$ でかつ $i_j>k$ となるものが存在する．C_k の元に対して，もし (i) が成りたてば，その元は C_{k+1} の元であり，もし (ii) が成りたてば，$c_w, c_k, \cdots, c_k, c_t, \omega>k, t>k$ を書かれた各部分に対して，それに，$((\cdots(c_w, c_k), \cdots), c_k)c_t$ という具合に括弧をつけることにより，C_{k+1} の元が一意的に定まる．逆に，C_{k+1} に属する元に対しては，c_k をうしろに含む括弧をすべて取り去ることにより，C_k の元が一意的に定まる．したがって，このようにして，C_k と C_{k+1} の間に 1 対 1 の対応がついた．いま，k を十分大きくとれば，交換子 c_k の重さは n より大きくなり，したがって (ii) は起こり得ない．したがって，括弧づけを続けていくことにより，最後には (i) が成り立つようになる．ここで，各語は重さ n の基本積であるか，または重さ d の同じ基底交換子を $s=n/d$ 個並べたもののいずれかである．括弧をつけて，C_k の元

から C_{k+1} の元を決めるときに，新しく作った一くくりの括弧の中には1つの c_w といくつかの c_k が存在する．したがって各括弧は，ある最小の巡回部分に完全に含まれる．したがってすべての最小の巡回部分はこのような括弧を含んでいる．したがって任意の語に対してそこに現われる巡回部分の個数は，括弧をつける各段階において不変に保たれる．したがって，長さ n の巡回語に括弧をつけることにより，重さ n の基底交換子全部と，各 $d|n$ に対して重さ d の同じ基底交換子を n/d 個ならべたもの全部が現われる．なぜならば，k を十分大きくとったとき，これらの元は C_k に含まれているからである．したがって補題の証明は完成した．

長さ n かつ周期 n の巡回語はいくつ存在するか？　このことを次に考える．長さ n，周期 d，$d|n$，の一つの巡回語から次の d 個の通常の語が生ずる．

$$a_1\cdots\cdots\cdots a_d a_1\cdots\cdots\cdots\cdots a_d\cdots\cdots\cdots a_d a_1\cdots\cdots a_d$$
$$a_2\cdots\cdots a_d a_1 a_2\cdots\cdots\cdots a_d a_1\cdots\cdots a_d a_1 a_2\cdots a_d a_1$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_d a_1\cdots a_{d-1} a_d a_1\cdots\cdots a_{d-1}\cdots\cdots a_{d-1} a_d\cdots a_{d-1}$$

したがって，長さ d かつ最小の周期 d の巡回語の個数は $M_r(d)$ であり，r^n 個の通常の語に対して一意的に最小の周期 d が定まるから，

(11.2.7) $$r^n = \sum_{d|n} dM_r(d)$$

である．

一方，Möbius の反転公式は，もし

(11.2.8) $$f(n) = \sum_{d|n} g(d)$$

であれば，

(11.2.9) $$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$$

であることを主張する．したがって (11.2.7) に Möbius の反転公式*) を適用すれば，

---

*) Hardy and Wright 〔1〕 p. 235

$$nM_r(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)r^{n/d}$$

すなわち,

(11.2.10) $$M_r(n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)r^{n/d}$$

である.(Witt の公式)

一方, $\omega_i(W)=n_i,\ n_1+\cdots+n_r=n$ を満たす通常の語 W の個数は, 多項係数

$$\frac{n!}{n_1!\cdots n_r!}$$

である. このことから, 次の式

(11.2.11) $$\frac{n!}{n_1!\cdots n_r!}=\sum_{d|n_1,\ \ ,n_r}dM\left(\frac{n_1}{d},\frac{n_2}{d},\cdots,\frac{n_r}{d}\right)$$

が導びかれる. ここで d は $n_1,\cdots,n_r$ の最大公約数 n_0 の約数をすべて動く. したがって, Möbius の反転公式を適用すれば,

(11.2.12) $$M(n_1,n_2,\cdots,n_r)=\frac{1}{n}\sum_{d|n_1,\cdots,n_r}\mu(d)\frac{\left(\frac{n}{d}\right)!}{\left(\frac{n_1}{d}\right)!\cdots\left(\frac{n_r}{d}\right)!}$$

を得る.(Witt の第二公式)

r 個の生成元 $x_1,x_2,\cdots,x_r$ から生成された整数係数の自由結合環 R を考える. 次数 m の元全体 R_m は, 加法に関して r^n 個の積 ($x_1,x_2,\cdots,x_r$ の r 個の積) $x_{i_1}\cdots x_{i_m}$ 達を基底とする自由アーベル群を作る. 一般に結合環において, 交換子 $[u,v]$ を

(11.2.13) $$[u,v]=uv-vu$$

で定義する. 交換子, 基底交換子, 基本積等は, 環 R においても群の場合と同様にして定義される. また群の交換子に関するいままで行なってきた種々の形式的な議論は環の交換子に対しても成り立つ. 群における交換子と環における交換子は種々の点において密接な関係がある. これについては Magnus [1] が最初の論文である.

定理 11.2.3. 次数 m の基本積達は, R_m の加法に関しての基底を作る.

系 11.2.1. 次数mの基底交換子達は一次独立である.

証：定理11.2.1により，次数mの（環の）基本積の個数はr^mである．これはR_mの基底の個数に等しい．したがって，R_mの任意の元が基本積達の整数係数の一次結合で表わされることを示しさえすればよい．いま，$P_1^{(m)}=P_1$はr^m個の積 $x_{i_1}\cdots x_{i_m}$ 達からなる基底であり，kが十分大きいときにはP_kは基本積だけからなる．したがって，P_kの任意の元がP_{k+1}の元の整数係数の一次結合で表わされることを示しさえすればよい．いま，簡単のために，次の記号を用いる．

$$[[\cdots[[u, v], v]\cdots], v]=[u, \overbrace{v, \cdots, v}^{s}]=[{}^s u, v^s]$$

（ここで，s個のvが存在する.）ところで，次の恒等式が後で必要となる．

$$uv^s=v^s u+\sum_{j=1}^{s}\binom{s}{j}v^{s-j}[{}^j u, v^j]. \tag{11.2.14}$$

$s=1$ のとき，この恒等式は

$$uv=vu+[u, v]$$

となり明らかに成り立つ．ところで，一般に恒等式

$$[{}^j u, v^j]v=[{}^{j+1}u, v^{j+1}]+v[{}^j u, v^j] \tag{11.2.15}$$

が成り立つ．そこで，(11.2.14) はsに関する帰納法を用いて証明される．すなわち，(11.2.14) の両辺に右からvを乗じ，(11.2.15) を用いて変形し，同じ項をまとめあわせれば，$s+1$ に対して (11.2.14) が成り立つからである．いま，P_kに $\cdots uc_k\cdots c_k w\cdots u$,（$w\neq c_k$, uはc_kより順番が後の基底交換子），という部分列を持つ元が含まれているとする．これに，$u=u, v=c_k$ として，(11.2.14) を適用する．そのようにして得られた元は，P_{k+1}に属するか，または元c_kの個数がもとに比べて減ったP_kの元か，またはc_kの位置がもとに比べて前に進んでいる．したがって，(11.2.14) を繰り返して適用すれば，任意のP_kの元はP_{k+1}の元の整数係数一次結合として表わされる．したがって定理の証明は完成した．

Rに単位元1を加え，有理整数を次数0の元の集合R_0とみなす．Rを，次数

$n+1$ 以上の元全体から生成された両側イデアルでわった商環を $\bar{R}$ で表わす．このとき，

(11.2.16) $$\bar{R}=R_0+R_1+\cdots+R_n$$

である．$\bar{R}$ において，定数項が1である元，$1+z, z\in R_1+\cdots+R_n$，の全体は乗法に関して群 G を作る．なぜならば，$z^{n+1}=0$ だから，

(11.2.17) $$(1+z)^{-1}=1-z+z^2+\cdots+(-1)^n z^n$$

が成り立つからである．いま，$1+z=1+u_m+u_{m+1}+\cdots+u_n$, $u_j\in R_j(j=m, m+1,\cdots n,)$, $u_m\neq 0$ であるとき，u_m を元 $1+z$ の**先頭項** (leading term) とよぶ．元1の先頭項は0と置く．

補題 11.2.2. G の元 $u, v(u\neq 1, v\neq 1)$ の先頭項が各々次数 s, t の u_s, v_t であるとする．このとき，u^{-1}, v^{-1} の先頭項は $-u_s, -v_t$ である．uv の先頭項は，もし $s<t$ ならば，u_s, $t<s$ ならば v_t, $t=s$ かつ $u_s+v_t\neq 0$ ならば u_s+v_t である．また，環における交換子 $[u_s, v_t]$ が0でなければ，これは群 G の交換子 (u, v) の先頭項である．

証：$u=1+a$, $v=1+b$, $u^{-1}=1+a'$, $v^{-1}=1+b'$ と置く．このとき，

$$a+a'+aa'=0 \qquad aa'=a'a$$
$$b+b'+bb'=0 \qquad bb'=b'b$$
$$a=u_s+\cdots+u_n,\quad b=v_t+\cdots+v_n$$
$$uv=1+a+b+ab$$

である．これらの関係式から，u^{-1}, v^{-1}, uv の先頭項に関する主張が成り立つことは明らかである．また，これらの関係式から，

$$\begin{aligned}(u, v)&=u^{-1}v^{-1}uv\\&=(1+a')(1+b')(1+a)(1+b)\\&=1+ab-ba+aa'b-bb'a+b'ab+a'b'a+a'b'ab\end{aligned}$$

が成り立つ．したがって，

(11.2.18) $$(u, v)=1+[u_s, v_t]+\text{高次の項}$$

であり，補題の主張はすべて証明された．

Fを $y_1, y_2, \cdots, y_r$ から生成された自由群，$c_1, c_2, \cdots$ をFにおける基底交換子をならべたものとする．さらに，$d_1, d_2, \cdots$ を，$y_1, \cdots, y_r$ を $x_1, \cdots, x_r$ で置き換えることによって得られた，自由結合環Rにおける（環としての）交換子をならべたものとする．また，重さnの基底交換子でその順番が一番後のものをc_tとする．このとき，c_i 達とRの元 d_j 達の間に次のような対応が存在する．

補題 11.2.3. 対応 $y_i \to 1+x_i (i=1, \cdots, r)$ によりFからGの上への写像が定まる．この写像による c_i の像を $g_i \in G (i=1, 2, \cdots, t)$ とする．このとき，g_i の先頭項は d_i である．

証：$y_i \to 1+x_i (i=1, \cdots, r)$ だから，$g_i = 1+x_i$ の先頭項は $x_i (i=1, \cdots, r)$ である．いま，帰納法を用いてこの補題を証明する．もし $c_w = (c_u, c_v), \omega \leqq t$ であれば，帰納法仮定により g_u の先頭項は d_u，g_v の先頭項は d_v である．したがって，補題11.2.2により，(g_u, g_v) の先頭項は（もし $[d_u, d_v]$ が0でなければ）$[d_u, d_v]$ である．が，これは系11.2.1により0でない．したがって $g_w = (g_u, g_v)$ の先頭項は $[d_u, d_v] = d_w$ であり，証明は完成した．

定理 11.2.4.（基底定理）*) Fを $y_1, \cdots, y_r$ から生成された自由群，$c_1, c_2, \cdots, c_t$ をFの重さn以下の基底交換子をならべたものとする．このとき，Fの任意の元fは，

(11.2.19) $$f = c_1^{e_1} c_2^{e_2} \cdots c_t^{e_t} \bmod F_{n+1}$$

と一意的に表わされる．さらに，重さnの基底交換子達は自由アーベル群 F_n/F_{n+1} の基底をなす．

証：第二の主張から先に証明する．いま，$c_s, \cdots, c_t$ を重さnの基底交換子達の全体とする．補題11.2.3により，

(11.2.20) $$y_i \to 1+x_i = g_i \ (i=1, \cdots, r)$$

で定義された写像による $c_s, \cdots, c_t$ の像である（環における）交換子達の先頭項はそれぞれ次数nの基底（環）交換子 $d_s, \cdots, d_t$ である．定理11.2.3によ

---

*) Marshall Hall, Jr. [6] 参照.

り，これら $d_s, \cdots, d_t$ は一次独立である．また，補題 11.2.2 により，$c_s^{e_s}\cdots c_t^{e_t}$ の先頭項は $e_sd_s+\cdots+e_td_t$ であり，$e_s=\cdots=e_t=0$ でない限り，これは 0 でない．したがって $c_s, \cdots, c_t$ は F_n/F_{n+1} の独立な元であり，したがって F_n/F_{n+1} の基底をなす．なぜならば，すでに (11.1.4) で示したように，F_n/F_{n+1} の任意の元は $c_s, \cdots, c_t$ の一次結合で表わされるからである．すでに (11.1.4) で示したように，f を (11.2.19) の形に表わす方法は少なくとも一つはある．

次にこの表わし方の一意性を示す．もし，

(11.2.21) $$c_1^{e_1}\cdots c_t^{e_t}=c_1^{h_1}\cdots c_t^{h_t} \pmod{F_{n+1}},$$

$h_i=e_i(i=1, \cdots j-1)$ かつ $h_j\neq e_j$ であれば，c_j の重さが k であるとき，mod F_{k+1} で考えたとき，重さ k の基底交換子達が一次従属となる．しかし，これは起こり得ない．したがって (11.2.18) の表わし方は一意的である．これで，証明は完成された．

第12章　p-群と正則 p-群

12.1. 初等的な結果

第4章および第10章で，有限 p-群 P に関していくつかの初等的な性質を示したが，それらをここに整理しよう．

1)　P の中心 Z は単位元以外の元を含む（定理 4.3.1)

2)　P の真部分群 H の正規化群は H 自身に一致しない（定理 4.2.1).

3)　P の位数が p^n ならば，すべての極大部分群 M は位数が p^{n-1} でかつ正規部分群である．(定理 4.3.2)

4)　P の位数 p の部分群は P の中心に含まれる．(定理 4.3.4)

5)　P は超可解（super solvable）である．(定理 10.3.4 と定理 10.2.4)

6)　P は巾零（nilpotent）である。(定理 10.3.4)

12.2. Burnside の基底定理．p-群の自己同型

群 P の位数を p^n とする．このとき，その極大部分群すべての共通部分 D は特性部分群である．この D を P の **Frattini 部分群**とよぶ．このとき準同型写像 $P \to P/D$ により，P を生成する元の集合は，P/D を生成する元の集合の上に写される．このことの逆も，次に示すように，強い意味において成り立つ．これが次の Burnside の基底定理の主題である．

定理 12.2.1. (**Burnside 基底定理**) D を p-群 P のすべての極大部分群の共通部分とする(すなわち，D は P の Frattini 部分群)．このとき商群 $P/D=A$ は初等アーベル群である．A の位数が p^r であれば，P を生成する任意の集合 $z_1, \cdots, z_s$ の中から，P を生成する r 個の元 $x_1, \cdots, x_r$ を選ぶことができる．準同型写像 $P \to A$ により，$x_1, \cdots, x_r$ は A の基底 $a_1, \cdots, a_r$ の上に写される．

逆に r 個の P の元の集合に対して写像 $P\to A$ によるその像の集合が A を生成するならば，この r 個の元は P を生成する．

証：M を P の 1 つの極大部分群とすれば，M は指数 p の正規部分群である．したがって，P/M は位数 p の巡回群である．したがって，P の各元の p 巾および（P の）すべての交換子は M に含まれる．したがって，D（すべての極大部分群の共通部分）も各元の p 巾，および各交換子をすべて含む．よって $P/D=A$ は初等アーベル群である．いま A の位数が p^r であれば，A のすべての基底は r 個の元からなる．いま，集合 $b_1, \cdots, b_s$ が A を生成すれば，これ等 b_i のうち，1 と等しいものおよび $b_1, \cdots, b_{i-1}$ により生成される A の部分群に含まれるものを除くことにより，新しく A を生成する部分集合 $a_1, \cdots, a_r$ が得られ，$s\geq r$ である．

さて，$z_1, \cdots, z_s$ が P を生成すると仮定しよう．写像 $P\to P/D=A$ により，$z_i\to b_i$ $(i=1, \cdots, s)$ であるとする．このとき $b_1, \cdots, b_s$ は A を生成する．したがって A の基底である部分集合 $a_1, \cdots, a_r$ を含む．いま $x_1, \cdots, x_r$ を $x_i\to a_i$ なる $z_1, \cdots, z_s$ の部分集合とする．さて，A のある 1 つの基底 $a_1, \cdots, a_r$ の上に写される P の元からなる任意の集合 $x_1, \cdots, x_r$ が P を生成することがいえれば，定理の証明は完成するわけである．$H=\{x_1, \cdots, x_r\}$ と置く．もし $H\neq P$ であれば H は P のある極大部分群 M に含まれる．しかし，その場合には，写像 $P\to P/D=A$ により，$H\to HD/D\subseteq M/D=B$（ここで B は位数 p^{r-1} の A のある部分群）である．これは $H=\{x_1, \cdots, x_r\}\to\{a_1, \cdots, a_r\}=A$ であることに矛盾する．したがって $H=P$ であり $x_1, \cdots, x_r$ は P を生成する．証終．

この定理を応用して，P の自己同型群 $A(P)$ に関して，いくつかのことが分かる．いま，P/D の基底 $a_1, \cdots, a_r$ の選び方は $\theta(p^r)=(p^r-1)(p^r-p)\cdots(p^r-p^{r-1})$ 通りである．なぜならば a_1 として単元位と異なる p^r-1 個のどの元でも選ぶことができ，$a_1, \cdots, a_i$ まで選んでしまった後では a_{i+1} として $a_1, \cdots, a_i$ で生成される部分群に属さない p^r-p^i 個のどの元でも選べるからである．したがって，A の基底として $\theta(p^r)$ 通りの選び方がある．一方，一つ

の固定した基底 $a_1, \cdots, a_r$ を他の基底 $b_1, \cdots, b_r$ に写す写像は A の自己同型を引き起こす．逆にAの各自己同型は基底 $a_1, \cdots, a_r$ をやはり基底の上に写す．したがって全部でちょうど $\theta(p^r)$ 個のAの自己同型が存在する．

さて，順序づけられたr個の元 x_i 達からなる集合 $X=(x_1, \cdots, x_r)$ でPを生成するものの個数はちょうど $p^{r(n-r)}\theta(p^r)$ である．なぜならば，XからAの基底の上への写像 $x_i \to a_i (i=1, \cdots, r)$ において，Aの基底として $\theta(p^r)$ 通りの選び方があり，また各 a_i に対して，a_i に写されるDによる1つの剰余類が p^{n-r} 個の元を含むからである．Pの各自己同型は（順序づけられた）集合Xをやはりある（順序づけられた）集合に写す．したがって，Pの自己同型群$A(P)$はX達の上での置換群であると考えることができる．一方1つの（順序づけられた）集合Xを固定するPの自己同型はx達からなる積をすべて固定するから群Pを完全に固定する．すなわち恒等変換である．したがって，$A(P)$はX達の上で正則（な置換群）である．したがって，$A(P)$による各可遷域の長さは $A(P)$ の位数（$=k$ とおく）と等しい．したがって，$p^{r(n-r)}\theta(p^r)=kt$ が成り立つ．ここで，数tはr個の元でPを生成するときの本質的に異なる方法の個数であると解釈することができる．ここで，2つの集合 $X=(x_1, \cdots, x_r)$ と $Y=(y_1, \cdots, y_r)$ が本質的に同じ方法でPを生成するとは，各関係 $w(x_1, \cdots, x_r)=1$ に対して $w(y_1, \cdots, y_r)=1$ が成り立ち，また逆も成り立つことを言う．

いま A/D の各元を固定する自己同型からなる $A(P)$ の正規部分群を$A_1(P)$と置く．このとき群 $A_1(P)$ は，準同型写像 $P \to P/D=A$ によりAの同一の基底 $a_1, \cdots, a_r$ 上に写される $p^{r(n-r)}$ 個の（Pを生成する）集合 $X=(x_1, \cdots, x_r)$ 達の上に正則に作用する．したがって $A_1(P)$ の位数は $p^{r(n-r)}$ を割る．以上のこと（P. Hall [2] による）をまとめて，次の定理を得る．

定理 12.2.2. Pを位数 p^n の p-群，DをPの極大部分群全体の共通部分，$[P:D]=p^r$ とするとき，Pの自己同型群 $A(P)$ の位数は $p^{r(n-r)}\theta(p^r)$ を割る．また，P/D の各元を固定する（Pの）自己同型全体の作る群 $A_1(P)$ の位数は

$p^{r(n-r)}$ を割る.

12.3. 集 中 公 式

Gを元 $a_1, \cdots, a_r$ から生成された群とする．元 $(a_1 \cdot a_2 \cdots a_r)^n$ を $a_1, a_2, \cdots, a_r$ の高次の交換子を用いて表わすことが以下の目標である．いま，G が $a_1, a_2, \cdots, a_r$ から生成される自由群であると仮定してもかまわない．なぜならば，もしその自由群に対して成り立つ公式が得られれば，その公式は自動的に r 個の元から生成された任意の群に対しても成り立つからである．

§11.1 で述べた基底交換子の定義をもう一度繰り返して述べる．ただしここでは，順序をもっと詳しく定める．

1) $a_1, \cdots, a_r$ は重さ 1 の基底交換子である．$a_1 < a_2 < \cdots < a_r$ と順序を定める．

2) 重さ $n-1$ 以下の基底交換子とその順序が定まったとき，重さ n の基底交換子を次のようにして定める．すなわち，(x, y) が次の 3 条件 a), b), c) を満たしているとき重さ n の基底交換子という．

(a) x, y は基底交換子で $\omega(x)+\omega(y)=n$

(b) $x>y$

(c) $x=(u, v)$ ならば $y \geqq v$

3) 重さ n の交換子の順序は重さ $n-1$ 以下の交換子の後に位置する．2 つの重さ n の交換子 (x_1, y_1) と (x_2, y_2) に対して $y_1 < y_2$, または $y_1 = y_2$ かつ $x_1 < x_2$ であるとき $(x_1, y_1) < (x_2, y_2)$ と定義する．

さて，

(12.3.1) $$(a_1 a_2 \cdots a_r)^n = a_1^{(1)} a_2^{(1)} \cdots a_r^{(1)} a_1^{(2)} \cdots a_r^{(2)} \cdots a_r^{(n)}$$

なる形の G の元を考える．ここで，各生成元 a_i に対して上の式のどの位置にあるのかを区別するために，左から右へ $a_i^{(1)}, a_i^{(2)}, \cdots, a_i^{(n)}$ と番号をふってある．交換子の定義により $SR=RS(S, R)$ が成り立つ．したがって，(12.3.1) の表現で連続した元の組 SR を $RS(S, R)$ で置き換えれば，G における同一の元の異なった表現が得られる．この置き換えを繰り返すことにより，任意の

文字を好きなだけ左へ持っていくことができる．そこで，式（12.3.1）を次に定める特殊な方法にしたがって変形させる．まず，$a_1^{(2)}$ を $a_1^{(1)}$ の直後にくるまで左に動かす．次に $a_1^{(3)}$ を $a_1^{(2)}$ の直後にくるまで左に動かす．この操作を続けてすべての文字 a_1 達を左端に持ってくる．これで集中操作の第一段階が終る．次に，a_2 達をその番号の順にすべてが a_1 達にすぐ続くように左に集める．以下同様にしてこの操作を続ける．

もう少し詳しくこの集中操作について考察しよう．第 i 段階が終ったとき（すなわち i 番目以下の基底交換子をすべて左に移し終えたとき）

(12.3.2)
$$(a_1a_2\cdots a_r)^n=c_1^{e_1}c_2^{e_2}\cdots c_i^{e_i}R_1R_2\cdots R_t$$

であるとする．ここで $c_1,\cdots,c_i$ は1番目から i 番目までの基底交換子を表わし，$R_1,\cdots,R_t$ は順序が c_i の後にある基底交換子を表わす．いま $R_1,\cdots,R_t$ のうちで c_{i+1} に等しいものを $R_{j_1},R_{j_2},\cdots,R_{j_s}$（添字の小さい順にならべる）とする．まず R_{j_1} を $c_i^{e_i}$ の直後にくるまで左へ移す．次に $R_{j_2},R_{j_3},\cdots$，最後に R_{j_s} を左へ移す．したがって $e_{i+1}=s$ であり（12.3.2）は次の形に変わる．

(12.3.3)
$$(a_1a_2\cdots a_r)^n=c_1^{e_1}c_2^{e_2}\cdots c_{i+1}^{e_{i+1}}R_1^*\cdots R_k^*$$

これで第 $i+1$ 段階が終了する．

式（12.3.2）において，$c_1^{e_1}\cdots c_i^{e_i}$ を集中部分，$R_1\cdots R_t$ を非集中部分とよぶ．しかし，この定義が意味を持つためには，各段階の式において基底交換子のみが現われることを証明しなければならない．0段階の最初の式（12.3.1）は確かに重さ1の基底交換子だけからできている．いま，帰納法により，第 i 段階が終ったとき，非集中部分 $R_1\cdots R_t$ は（順序が c_i より後の）基底交換子だけからできていると仮定する．いま集中操作をほどこして c_{i+1} と等しいある R_j $(1\leq j\leq t)$ を左へ移すとき新しく現われる交換子は $(c_j,c_{i+1},\cdots,c_{i+1})(j\geq i+2)$ という形のものばかりである．これらの交換子はいずれも基底交換子である．なぜならば，もし $c_j=(c_r,c_s)$ であれば c_j は c_s が集中操作の適用をうける第 s 段階に現われる．したがって，$s<i+1$ であり，$c_s<c_{i+1}$，したがって (c_j,c_{i+1}) は基底交換子である．したがって（$c_j,c_{i+1},\cdots,c_{i+1}$）も基底交換子である．すでに（12.3.1）において見たように生成元 a_i に対して $a_i^{(j)}(j=1,\cdots,n)$ と

番号をつけた．いま，重さ w_1 の交換子 R の番号が $(\lambda_1, \cdots, \lambda_{w_1})$，重さ w_2 の交換子 S の番号が $(\mu_1, \cdots, \mu_{w_2})$ であるとき，交換子 (R, S) に番号 $(\lambda_1, \cdots, \lambda_{w_1}, \mu_1, \cdots, \mu_{w_2})$ を割りふることにする．(12.3.3) における指数 $e_1, \cdots, e_i, e_{i+1}$ はこれらの番号を用いて計算される．ここで $e_{i+1}=s$ は第 i 段階終了時における非集中部分の中の c_{i+1} と等しい交換子の個数である．したがって，その個数は第 i 段階終了時における c_{i+1} と等しい交換子の個数（$=E_{i+1}$ と置く）と等しい．また，もし $c_{i+1}=(c_r, c_s)$ であれば，この c_{i+1} はこの特別な c_r が，この特別な c_s の前にあるときに c_s が集中操作の適用を受けるときに現われる．したがって，まず，非集中部分に含まれる2つの交換子 c_r と c_s に対して，c_r が c_s の直前にあるのはいつか？　という問を考える．

第0段階においては，重さ1の交換子が存在して，他の重さの交換子は存在しない．このとき，明らかに，各番号 $\lambda=1, \cdots, n$ に対して $a_k^{(\lambda)}$ は存在する．さらに第0段階において $a_r^{(\lambda)}$ が $a_s^{(\mu)}$ に先行するための必要十分条件は，$r \geq s$ ならば $\lambda<\mu$, $r<s$ ならば $\lambda \leq \mu$ であることである．したがって第0段階において，$a_k^{(\lambda)}$ が存在するという存在条件 $E_k{}^0$ および $a_r^{(\lambda)}$ が $a_s^{(\mu)}$ に先行しているという先行条件 $P_{rs}{}^0$ は次に定義する (L)-条件である．すなわち，整数の集合 $\lambda_1, \cdots, \lambda_m$ に対して，$\lambda_t<\lambda_u, \lambda_t \leq \lambda_u$ といういくつかの関係からなっているような条件を (L)-条件とよぶ．さて，次に，第 i 段階終了時に符号が $(\lambda_1, \cdots, \lambda_m)$ である交換子 c_k が存在するという条件 $E_k{}^i$ は，$\lambda_1, \cdots, \lambda_m$ に関する (L)-条件であり，また，第 i 段階終了時の非集中部分において符号が $(\lambda_1, \cdots, \lambda_m)$ の交換子 c_r が符号が $(\mu_1, \cdots, \mu_q)$ の交換子 c_s に先行するという条件 $P_{rs}{}^i$ は $\lambda_1, \cdots, \lambda_m, \mu_1, \cdots, \mu_q$ に対する (L)-条件であるということを i（段階）に関する帰納法を用いて証明する．第0段階に対する存在条件 $E_k{}^0$ および先行条件 $P_{rs}{}^0$ が (L)-条件であることはすでに示した．いま $E_k{}^i$ および $P_{rs}{}^i$ が (L)-条件であると仮定する．このとき，$E_k{}^{i+1}$ および $P_{rs}{}^{i+1}$ が (L)-条件であることを次に示す．さて，(12.3.2) と (12.3.3) を比較する．$R_{j_1}=R_{j_2}=\cdots=R_{js}=c_{i+1}$ に対して，まず R_{j_1} に集中操作をほどこし，次に R_{j_2} に……，最後に R_{j_s} にほどこす．ところで集中操作は $SR=RS(S, R)$ という置き換え

を繰り返すだけである．したがって，第 i 段階終了時に存在する c_{i+1} と異なる任意の交換子は第 $(i+1)$ 段階終了時において存在し，順序も不変に保たれる．したがってそのような交換子に対しては $E_k^{i+1}=E_k^i$, $P_{rs}^{i+1}=P_{rs}^i$ である．したがって，あとは，$(i+1)$ 段階において初めて現われる交換子 c_k の存在条件と，c_r, c_s のいずれか（あるいは両方）が $(i+1)$ 段階において初めて現われるときの先行条件 P_{rs}^{i+1} についてのみ考えれば良い．第 $(i+1)$ 段階において現われる交換子は，$c_k=(c_j, R_{u_1}, \cdots, R_{u_m})$ という形をしている．これは，R_{u_1} が c_j を越え，R_{u_2} がその交換子を越え，……，R_{u_m} が $(c_j, R_{u_1}, \cdots, R_{u_{m-1}})$ を越えたときに現われる．ここで $R_{u_1}, \cdots, R_{u_m}$ はいずれも c_{i+1} と等しいとする．したがって，存在条件 E_k^{i+1} は，$c_j, R_{u_1}, \cdots, R_{u_m}$ の存在条件と，それらが第 i 段階終了時に上の順序通りに並んでいるという先行条件との論理的な積として表わされる．したがって E_k^{i+1} は c_k の番号達に対する (L)-条件である．第 $(i+1)$ 段階において集中操作を行なうとき，交換子 (S, R) は，$SR=RS(S, R)$ として S の直後かつ S につづく交換子達の前に現われる．さて，$c_r=c_{j_1}$ または $(c_{j_1}, R_{u_1}, \cdots, R_{u_m})$ であり，かつ $c_s=c_{j_2}$ または $(c_{j_2}, R_{v_1}, \cdots, R_{v_w})$ であるときの先行条件 P_{rs}^{i+1} について考えよう．いま，$c_{j_1}\neq c_{j_2}$ ならば，$P_{rs}^{i+1}=P_{j_1j_2}^i$ である．しかし，もし $c_{j_1}=c_{j_2}$ ならば，P_{rs}^{i+1} が R 達を含むことが起こりうる．いま，e を $R_{u_1}=R_{v_1}, \cdots, R_{u_e}=R_{v_e}$ となる最大の整数とする．このとき，c_r が c_s に先行するためには，（1）$m=e$ でかつ $R_{u_{e+1}}$ が存在しない（このとき c_s は c_r の交換子となる）または（2）$R_{v_{e+1}}$ が $R_{u_{e+1}}$ に先行する，のいずれかでなければならない．したがって，ある符号 c_r がある符号 c_s に先行するという先行条件 P_{rs}^{i+1} はいくつかの先行条件達の論理的な積として表わされ，したがって (L)-条件である．

補題 12.3.1. 与えられた (L)-条件を満たす整数 $\lambda_1, \cdots, \lambda_m, 1\leq\lambda_i\leq n$ の組の個数は $b_1n+b_2n^{(2)}+\cdots+b_mn^{(m)}$ である．ここで $n^{(i)}=n(n-1)\cdots(n-1+i)/i!$ であり，b は 条件 (L) のみにより定まる（n によらない）自然数である．

証：添字 $1, 2, \cdots, m$ からなる集合を共通部分を持たない部分集合 $S_1, S_2,$

$\cdots, S_t$ の和にわける．このとき，$\lambda_1, \cdots, \lambda_m$ に対する順序を $\lambda_j = v_i$ ($j \in S_i$, $i=1, \cdots, t$ ここで $v_1 < v_2 < \cdots < v_t$) で与える．さて可能な λ_j の選び方はいずれもこのようにして得られる．また v 達の選び方には $n^{(t)}$ 通りの方法がある．これは n 個の中から t 個を選ぶ組み合わせの個数である．さて，このようにして λ 達を1つ決めたとき，それは (L)–条件を満たすか満たさないかのいづれかである（v 達のとり方によらずに決まる）．したがって，(L)–条件を満たす λ 達の解の個数は $b_1 n + b_2 n^{(2)} + \cdots + b_m n^{(m)}$ と表わされる．ここで b_t は (L)–条件を満たす順序づけられた t 個の異なる値の個数である．b_t は (L)–条件に依存するが n にはよらない．

たとえば，もし $\lambda_1, \lambda_2, \lambda_3$ が (L)–条件 $\lambda_1 < \lambda_2, \lambda_3 \leq \lambda_2$ を満たせば，それ等は

1) $\lambda_1 = v_1,\ \lambda_2 = \lambda_3 = v_2,\ v_1 < v_2$

2) $\lambda_1 = \lambda_3 = v_1,\ \lambda_2 = v_2,\ v_1 < v_2,$

3) $\lambda_1 = v_1,\ \lambda_1 = v_2,\ \lambda_2 = v_3,\ v_1 < v_2 < v_3$

4) $\lambda_3 = v_1,\ \lambda_1 = v_2,\ \lambda_2 = v_3,\ v_1 < v_2 < v_3$

のいずれかであり，この (L)–条件を満たす $\lambda_1, \lambda_2, \lambda_3$ の組の個数は $2n^{(2)} + 2n^{(3)}$ である．

すでに示したように，(12.3.2) における交換子 c_i の指数 e_i は第 $i-1$ 段階終了時における非集中部分の中の c_i に等しい交換子の個数に等しい．さらに，この個数はある (L)–条件を満たす整数の組 $\lambda_1, \cdots, \lambda_m$ の個数に等しい．ここで m は c_i の重さである．したがって補題 12.3.1 により，次の定理が成り立つ．

定理 12.3.1. $(a_1 a_2 \cdots a_r)^n$ に集中操作をほどこして，

$$(a_1 a_2 \cdots a_r)^n = a_1{}^n a_2{}^n \cdots a_r{}^n c_{r+1}{}^{e_{r+1}} \cdots c_i{}^{e_i} R_1 \cdots R_t$$

とできる．ここで，$c_l = a_l (l=1, 2, \cdots, r), c_{r+1}, \cdots, c_i$ は i 番目までの基底交換子を順番にならべたもの，$R_1, \cdots, R_t$ は順番が c_i より後の基底交換子である．$j (1 \leq j \leq i)$ に対して，指数 e_j は $e_j = b_1 n + b_2 n^{(2)} + \cdots + b_m n^{(m)}$ という形をしている．ここで m は c_j の重さであり，$b_1, b_2, \cdots, b_m$ は n のみによる（c_j によ

らない）自然数であり，$n^{(k)}=n(n-1)\cdots(n-k+1)/k!$ である．

さて，Gがクラスp以下の p-群であるときには．次の重要な系が得られる．重さp以下のすべての交換子に集中操作を適用し終えたとき，非集中部分は単位元のみからなる．さらに，$n=p^{\alpha}$ と置いたとき，すべての指数は p^{α} の巾である．なぜならば2項係数 $n^{(i)}(i\leq p-1)$ の分子はnの倍数であるが分母に現われる個数は $p-1$ を越えないからである．したがって次の系が成り立つ．

系 12.3.1. Pをクラスがp以下の p-群，$n=p^{\alpha}$ とする．このとき，

$$(a_1a_2\cdots a_r)^n=a_1{}^na_2{}^n\cdots a_r{}^nS_1{}^nS_2{}^n\cdots S_t{}^n$$

と表わされる．ここで $S_1, S_2, \cdots, S_t$ は $a_1, a_2, \cdots, a_r$ から生成される部分群の交換子群に属する元である．

12.4. 正則 p-群 (Regular p-Groups)

p-群Pが正則であるとは，任意の2元 a, b と任意の $n=p^{\alpha}$ に対して交換子群に属する元 $S_1, S_2, \cdots, S_t$ を適当に取ることにより

$$(ab)^n=a^nb^nS_1{}^n\cdots S_t{}^n \tag{12.4.1}$$

が成立することをいう．この定義と定理12.3.1の系12.3.1から直ちに分かるように，

1) クラスがpより小さい p-群は正則である．

2) 位数がたかだか p^p の p-群は正則である．

3) p-群 P の任意の2元から生成される部分群が常に正則ならば P は正則である．

4) 正則な p-群の部分群，商群はすべて正則である．

任意のpに対して位数 p^{p+1} の正則でない群が存在する．すなわち，p^2 個の文字の上の対称群 S_{p^2} の Sylow 群 $S^{(p)}$ がそれである．なぜならば，この群は位数pの2つの元から生成され，しかも位数 p^2 の元を含んでいるが，正則な群に対してはこのようなことが起こらないことが示されるからである．

定理 12.4.1. 正則 p-群Pにおいて（ここで $n=p^{\alpha}$ とする），a, b で生成される部分群 $H(a, b)$ の交換子群 $H_2(a, b)$ に属する元 S_1, S_2 を適当に選んで $a^n b^n=(ab)^n S_1{}^n=(abS_2)^n$ とすることができる．

系 12.4.1. 正則 p-群Pにおいて（ここで $n=p^{\alpha}$ とする）$H_2(a_1, \cdots, a_r)$ の元 S_1, S_2 を適当に選べば $a_1{}^n a_2{}^n \cdots a_r{}^n=(a_1 a_2 \cdots a_r S_2)^n=(a_1 \cdots a_r)^n S_1{}^n$ と表わすことができる．

証：$H(=H(a, b)$ または $H(a_1, \cdots, a_r))$ が アーベル群の場合には $S_1=1$, $S_2=1$ とおけば定理，系ともに成り立つ．次に群Hのすべての真部分群に関して定理，系が共に成り立っていると仮定したとき，Hに対して定理が成り立つことを帰納法を用いて示す．いま，Hが $a_1, \cdots, a_r$ から生成されていればHの交換子群 $H_2(a_1, \cdots, a_r)$ はHの真部分群であることに注意しよう．(12.4.1) により

$$a^n b^n=(ab)^n S_t{}^{-n} \cdots S_1{}^{-n}. \tag{12.4.2}$$

が成り立つ．帰納法の仮定により $S_t{}^{-n} \cdots S_1{}^{-n}=S^n$, $S \in H_2$ である．いま，$H=H(a, b)$ がアーベル群でなければ，H_2 と ab から生成される部分群はHの真部分群である．なぜならば，Burnside の基底定理により，もし H/H_2 が巡回群であればHも巡回群でなければならないからである．したがって帰納法の仮定によって $(ab)^n S^n=(abS_2)^n$ が成り立つ．すなわち，Hの各真部分群に対して定理および系が成り立つという仮定のもとに，Hに対して定理が成り立つことが証明された．次に，定理を $a_1{}^n a_2{}^n \cdots a_r{}^n$ に $r-1$ 回適用すれば，

$$a_1{}^n a_2{}^n \cdots a_r{}^n=(a_1 a_2 \cdots a_r)^n S_1{}^n \cdots S_{r-1}{}^n$$

$S_1, \cdots, S_{r-1} \in H_2$ が成り立つ．したがって $a_1{}^n a_2{}^n \cdots a_r{}^n=(a_1 a_2 \cdots a_r)^n S^n$ であり，系を H_2 に適用すれば，定理により，$(a_1 a_2 \cdots a_r)^n S^n=(a_1 a_2 \cdots a_r S_1)^n$ を得る．

定理 12.4.2. 有限 p-群Pが正則であるための必要十分条件は，Pの任意の2元 a, b に対して，a, b から生成される群の交換子群に属する元Sを選び

$$a^p b^p=(ab)^p S^p \tag{12.4.3}$$

とできることである.

証：(必要条件) これは定理 12.4.1 の特別な場合であるから明らかである.

(十分条件) 条件 (12.4.3) から

(12.4.4)　　$a^n b^n=(ab)^n S_1{}^n \quad (n=p^\alpha,\ S_1\in H_2(a,b))$

が導びかれることを示そう. さて, 関係

(12.4.5)　　$a_1{}^p a_2{}^p\cdots a_r{}^p=(a_1a_2\cdots a_r)^p S_1{}^p=(a_1a_2\cdots a_rS_2)^p$

$(S_1, S_2\in H_2(a_1,\cdots,a_r))$ はHがアーベル群のときには $S_1=S_2=1$ と置けば満たされる. もし(12.4.5)が任意の真部分群に対して成り立つならば (12.4.3) を $r-1$ 回適用して, $a_1{}^p a_2{}^p\cdots a_r{}^p=(a_1a_2\cdots a_r)^p u_1{}^p\cdots u_{r-1}{}^p$ とできる. (ここで $u_1,\cdots,u_{r-1}\in H_2$)このとき, 帰納法を用いて, $u_1{}^p\cdots u_{r-1}{}^p=S_1{}^p$ とできる. 一方, $b=a_1a_2\cdots a_r$ と S_1 はHの真部分群を生成する. したがって $(a_1a_2\cdots a_r)^pS_1{}^p=(a_1\cdots a_rS_2)^p$ であり, (12.4.5) が一般に成り立つことが示された.

補題 12.4.1. (12.4.3) を仮定するとき, Pの2元 x, y に対して, $H_2(x,y)$ の元Sが存在して, $x^{-p}y^{-p}x^py^p=S^p$ が成り立つ.

証： 仮定により,

$$x^py^p=(xy)^pS_1{}^p$$
$$y^px^p=(yx)^pS_2{}^p$$

とできる. したがって, $x^{-p}y^{-p}x^py^p=S_2{}^{-p}(yx)^{-p}(xy)^pS_1{}^p$. したがって

$$\begin{aligned}(yx)^{-p}(xy)^p&=(x^{-1}y^{-1}xy)^pS_3{}^p\\&=(x,y)^pS_3{}^p,\end{aligned}$$

ゆえに

$$x^{-p}y^{-p}x^py^p=S_2{}^{-p}(x,y)^pS_3{}^pS_1{}^p=S^p$$

が成り立つ. 補題証終.

この補題から直ちにわかるように, $a_1{}^p, a_2{}^p,\cdots,a_r{}^p$ からできている交換子は, $H_2(a_1,\cdots,a_r)$ のある元の p 乗となっている.

さて (12.4.3) から

(12.4.6)　　$a^{p^2}b^{p^2}=(a^pb^p)^pS_1{}^p$

$$=[(ab)^p S_2{}^p]^p S_1{}^p$$
$$=(ab)^{p^2} S_2{}^{p^2} S_3{}^p S_1{}^p$$

$S_1 \in H_2(a^p, b^p)$, $S_3 \in H_2((a,b)^p, S_2{}^p)$ とできる．補題で示したように，S_1, S_3 はいずれも $H_2(a,b)$ のある元の p 乗で表わされる．したがって

(12.4.7) $$a^{p^2} b^{p^2} = (ab)^{p^2} S_2{}^{p^2} S_4{}^{p^2} S_5{}^{p^2}$$

となる．したがって，帰納法により，$n=p^2$ に対して (12.4.4) が成り立つ．同様な方法により，補題を用いることによって，$n=p^\alpha$ の場合を仮定すれば $n=p^{\alpha+1}$ に対して (12.4.4) を示すことができる．

定理 12.4.3. Pが正則な p-群，$n=p^\alpha$ であれば

1) $(a^n, b)=1$ から $(a,b)^n=1$ が導かれ，また逆も成り立つ．

2) $(a^n, b)=1$ であれば $(a, b^n)=1$ である．

3) 元uを含む交換子Sの位数は，Pの中心を法としたときのuの位数を越えない．

4) 積 $a_1 a_2 \cdots a_r$ の位数は，$a_1, a_2, \cdots, a_r$ のいずれの元の位数をも越えない．

証：Pがアーベル群であれば，(1)，(2)，(3) は自明である．また (4) も明らかに成り立つ．次に，帰納法によって，P の任意の真部分群に対して (1)～(4) がいずれも成り立っていると仮定する．さらに P はアーベル群でないと仮定する．(12.4.4) を用いれば，

(12.4.8) $$a^{-n} b^{-1} a^n b = (a^{-1})^n (b^{-1}ab)^n = (a^{-1}b^{-1}ab)^n S^n$$

とできる．ここで $S \in K_2(a, b^{-1}ab) \subset H(a,b)$である，ここで$K=K(a, b^{-1}ab)$ $=H(a, b^{-1}ab)$ とおき $K_2=K_2(a, b^{-1}ab)$ でその交換子群を表わす．したがって

(12.4.9) $$(a^n, b)=(a,b)^n S_1{}^n$$

である．いま，$(a^n, b)=1$ であれば，$H(a,b)$ の中心を法として，元aの位数はnまたはそれ以下である．したがって $u=a$ とおくとき，真部分群 $K(a, b^{-1}ab)$ に対して性質 (3) が成り立つことから，Kにおける各交換子はaを含み，位数はたかだかnである．また (12.4.9) における元 S_1 はKにおける交換子の積として表わされる．Kに対して (4) が成り立つことから S_1 の位

数は高々 n であり，したがって $(a^n, b)=1$ から (12.4.9) において $S_1{}^n=1$ が導かれる．したがって $(a, b)^n=1$ が成り立つ．逆に，もし $(a, b)^n=1$ であれば，$K=K\ (a, a^{-1}b^{-1}ab)=K(a, u)$ （ここで $u=(a, b)$ である）の中心を法としたとき，u の位数は高々 n であり，各交換子は u を含む．K に対して(３)が成り立つことから，K_2 の交換子の位数はすべて高々 n である．また K_2 に対して（４）が成り立つことから，(12.4.9) における S_1 の位数は高々 n である．したがって $(a, b)^n=1$ から $S_1=1$ が導かれる．したがって $(a^n, b)=1$ である．よって P に対して（１）の成り立つことが示された．また（２)は(１)から直ちに導かれる．(１)を繰り返して適用すれば(３)が P において成り立つことが示される．なぜならば，もし P の中心を法としたときの u の位数が n であれば，もちろん $(u^n, v)=1$，したがって $(u, v)^n=1$ である．ところで $x=(u, v)$ と置けば $x^n=1$ だから $(x, y)^n=1$ である．

最後に P に対して性質（４）が成り立つことを示す．もし $a^n=1$, $b^n=1$ であれば，（３）により，a または b を含む任意の交換子の位数はたかだか n である．したがって，(12.4.4) において，S_1 は位数がたかだか n の交換子のいくつかの積として表わされる．真部分群 P_2 に対して性質（４）が成り立つことから S_1 はそれ自身位数はたかだか n である．したがって $S_1{}^n=1$ であり $(ab)^n=1$ である．それゆえ，２つの元の積の位数はそのどちらの元の位数をも越えない．したがって，これを繰り返せば，r 個の元の積の位数はそのいずれの元の位数をも越えないことが分かる．

定理 12.4.4. $n=p^\alpha$ のとき，$a^n=b^n$ であるための必要十分条件は $(ab^{-1})^n=1$ である．

証：定理 12.4.3 の性質（３）により，$H(a, b)$ におけるすべての交換子の位数はたかだか n である．したがって，$1=a^nb^{-n}=(ab^{-1})^nS_1{}^n$ において，$S_1{}^n=1$ であり，$(ab^{-1})^n=1$ が成り立つ．逆に，$a^nb^{-n}=(ab^{-1})^nS_1{}^n$，$(ab^{-1})^n=1$ であれば，$H(a, b)=H(a, ab^{-1})$ であり，$u=ab^{-1}$ としたとき，性質（３）により，$S_1{}^n=1$ である．したがって $a^n=b^n$ が成り立つ．

定理 12.4.5. 正則 p-群 P において, P の元の p 巾全体は特性部分群 $C^{\alpha}(P)$ を作る. また位数が p^{α} 以下の元全体は特性部分群 $C_{\alpha}(P)$ を作る.

証：$n=p^{\alpha}$ としたとき, 定理 12.4.1 における関係式, $a^n b^n=(abS_2)^n$ から, P の元の p 巾全体が部分群 $C^{\alpha}(P)$ を作ることがわかる. 明らかに $C^{\alpha}(P)$ は特性部分群であり, さらに全不変部分群である. また, 定理 12.4.3 の性質 (4) から, 位数が p^{α} 以下の元全体が部分群, したがって全不変部分群を作ることが導かれる.

12.5. 特殊な p-群, Hamilton 群

定理 12.5.1. 指数 p の巡回部分群を持った位数 p^n の群 P は次のいずれかである.

アーベル群

1) 巡回群. $a^{p^{n-1}}=1$, $n\geq 1$.

2) $a^{p^{n-1}}=1$, $b^p=1$, $ba=ab$, $n\geq 2$.

非アーベル群

3) $a^{p^{n-1}}=1$, $b^p=1$, $ba=a^{1+p^{n-2}}b$, p は奇数. $n\geq 3$.

4) 一般 4 元数群. $a^{2^{n-1}}=1$, $b^2=a^{2^{n-2}}$, $ba=a^{-1}b$, $p=2$, $n\geq 3$.

5) 二面体群. $a^{2^{n-1}}=1$, $b^2=1$, $ba=a^{-1}b$, $p=2$, $n\geq 3$.

6) $a^{2^{n-1}}=1$, $b^2=1$, $ba=a^{1+2^{n-2}}b$, $p=2$, $n\geq 4$.

7) $a^{2^{n-1}}=1$, $b^2=1$, $ba=a^{-1+2^{n-2}}b$, $p=2$, $n\geq 4$.

証：位数 p^n のアーベル群で, 位数 p^{n-1} の元を含むものの不変数は p^n または p^{n-1}, p である. したがってアーベル群の場合には定理の主張は正しい.

次に非アーベル群の場合を考える. まず, p を奇数と仮定する. 位数 p^{n-1} の元 a を 1 つ取ったとき, 部分群 $\{a\}$ は P の指数 p の正規部分群である. いま $b\notin\{a\}$ であれば, P が非アーベル群であることから, $bab^{-1}=a^r$, $r\not\equiv 1 \pmod{p^{n-1}}$ と表わされる. このとき, 任意の j に対して $ba^jb^{-1}=(bab^{-1})^j=a^{rj}$ で

あり，特に $j=r$ に対して $b^2ab^{-2}=b(bab^{-1})b^{-1}=ba^rb^{-1}=a^{r^2}$ であることに注意すれば，i に関する帰納法により，$b^iab^{-i}=a^{r^i}$ が得られる．いま，$b^p\in\{a\}$ だから，$b^pab^{-p}=a$ である．したがって $r^p\equiv1 \pmod{p^{n-1}}$ が成り立つ．いま p は奇数だから，この合同式から，$r\not\equiv1 \pmod{p^{n-1}}$に注意すれば，$r\equiv1+kp^{n-2} \pmod{p^{n-1}}$（ここで $k\not\equiv0 \pmod p$）が得られる．合同式 $ik\equiv1 \pmod p$ で定めた i に対して，$b_1=b^i$ と置く．このとき，$r^i\equiv(1+kp^{n-2})^i\equiv1+ikp^{n-2}\equiv1+p^{n-2} \pmod{p^{n-1}}$ である．したがって，$b_1ab_1^{-1}=b^iab^{-i}=a^{r^i}=a^{1+p^{n-2}}$ が成り立つ．そこで，$h=1+p^{n-2}$ と置く．このとき $(a^jb_1)^2=a^jb_1a^jb_1^{-1}b_1^2=a^{j(1+h))}b_1^2$ であり，帰納法により $(a^jb_1)^t=a^{jT}b^t$ が得られる．ここで $T=1+h+\cdots+h^{t-1}$ とする．p は奇数だから，$t=p$ に対して，$1+h+\cdots+h^{p-1}\equiv p+p^{n-2}[1+2+\cdots+(p-1)]\equiv p+p^{n-1}(p-1)/2\equiv p \pmod{p^{n-1}}$ が成り立つ．したがって $(a^jb_1)^p=a^{jp}b_1^p$ である．なお，この式は集中過程を用いても導くことができる．いま，$b_1^p=a^u\in\{a\}$ と表わす．このとき P は巡回群でないから b_1 の位数は p^n でなく，したがって $u=pv$ である．いま，$b_2=a^{-v}b_1$ と置けば，$b_2^p=(a^{-v}b_1)^p=a^{-vp}b_1^p=a^{-pv}a^{pv}=1$ であり，$b_2ab_2^{-1}=a^{-v}b_1ab_1^{-1}a^v=a^{-v}a^{1+p^{n-2}}a^v=a^{1+p^{n-2}}$ である．したがって a と b_2 は（3）で与えられている関係を満たす．

次に $p=2$ とし，位数 2^{n-1} の元を含む位数 2^n の非アーベル群を決めよう．$a^{2^{n-1}}=1, b\notin\{a\}$ とすれば，$bab^{-1}=a^r$ と表わされる．ここで $r^2\equiv1 \pmod{2^{n-1}}$，$r\not\equiv1 \pmod{2^{n-1}}$ である．この場合，r の取り方として，2^{n-1} を法として，$r=-1$，$r=1+2^{n-2}$，$r=-1+2^{n-2}$ の3通りがある．いま，$b^2=a^w\in\{a\}$ とすると，$b(b^2)b^{-1}=b^2$ だから $a^{wr}=a^w$，すなわち $wr\equiv w \pmod{2^{n-1}}$ が成り立つ．$r=-1$ とすれば $-w=w \pmod{2^{n-1}}$，したがって $a^w=1$ または $a^w=a^{2^{n-2}}$ である．したがって $r=-1$ のときは，P は（4）型の一般4元数群，または（5）型の二面体群であることがわかる．$n=3$ の場合には，§4.4で決定されているように，P はこれら（1）〜（5）の群のいずれかである．

次に $n\geq4$ かつ $ba=a^rb$，$r=1+2^{n-2}$ と仮定しよう．$b^2=a^w$ に関して，$wr\equiv w \pmod{2^{n-1}}$ の合同式は $2^{n-2}w\equiv0 \pmod{2^{n-1}}$ となる．したがって w は偶数であるから，$w=2w_1$ と表わされる．次に，合同式 $j(1+2^{n-3})+w_1\equiv0$

(mod 2^{n-2}) から j を定める．このとき，$b_1=a^jb$ に対して，$b_1{}^2=a^j(ba^j)b=a^{j(2+2^{n-2})}b^2=a^{2[j(1+2^{n-3})+w_1]}=a^{2^{n-1}}=1$ が成り立つ．すなわち，$b_1a=a^{1+2^{n-2}}b_1$ であり，a, b_1 は（6）の関係式を満たす．最後に，$n\geq 4$, $ba=a^rb$, $r=-1+2^{n-2}$ と仮定する．$b^2=a^w$ における w の条件 $w\equiv rw \pmod{2^{n-1}}$ は，$(2+2^{n-2})w\equiv 0 \pmod{2^{n-1}}$ すなわち $w=0 \pmod{2^{n-2}}$ となる．したがって $b^2=1$ または $b^2=a^{2^{n-2}}$ である．もし $b^2=a^{2^{n-2}}$ であれば，$b_1=ab$ と置けば $b_1{}^2=a(ba)b=a(a^{-1+2^{n-2}})b^2=a^{2^{n-2}}\cdot a^{2^{n-2}}=1$ が成り立つ．したがって a, b または a, b_1 のいずれかをとれば，それらは（7）の関係式を満たす．

定理 12.5.1 におけるすべての関係（1）～（7）はいずれも位数 p^n の群を定義する．このことは，一般 4 元数群の場合を除けば，定理 6.5.1 の方法を用いることにより示される．一般 4 元数群の場合には直接に証明することができる．これには後述の定理 15.3.1 を参照されたい．

定理 12.5.2. 位数 p の部分群がただ一つであるような p 群 P は巡回群または一般 4 元数群である．

証：n に関する帰納法を用いて定理を証明する．$n=1$ のときは明らかである．まず，p が奇数であると仮定する．帰納法の仮定により，P の指数 p の部分群 P_1 は巡回群である．したがって定理 12.5.1 により，p は奇数だから，P は（1），（2），（3）のいずれかの型である．しかし（2），（3）の型の群は明らかに位数 p の相異なる部分群を 2 つ以上含む．したがって P は（1）の型，すなわち巡回群である．次に，$p=2$ と仮定する．P が位数 2 の巡回部分群 P_1 を持てば，定理 12.5.1 により，P は（1），（2），（4），（5），（6），（7）のいずれかの型でなければならない．しかし P が（1）または（4）の型のとき，すなわち巡回群または一般 4 元数群，である場合を除けば，P は明らかに位数 2 の部分群を 2 つ以上含む．したがってあと残っている場合は，P の指数 2 の任意の部分群が一般 4 元数群の場合である．この場合は実際には起こり得ないことを次に示そう．

いま，$n\geq 4$ としてよい．まず $n=4$ の場合を考える．指数 2 の部分群 Q が

4元数群であるとする．c を Q に含まれない P の元とすれば，Q は $a^4=b^4=1$, $a^2=b^2$, $ba=a^{-1}b$ により与えられ，$P=Q+Qc$ である．元 c の位数は2巾だから，Qの3つの位数4の部分群 $\{a\}$, $\{b\}$, $\{ab\}$ の少なくとも1つは，c による変換で不変である．必要なら番号をつけかえて，そのような群が $\{a\}$ であるとしてよい．このとき，$c^{-1}ac=a$ または $c^{-1}ac=a^{-1}$ でなければならない．もし $c^{-1}ac=a$ であれば，$\{a, c\}$ はPにおける指数2のアーベル部分群だから，これは仮定に反する．もし $c^{-1}ac=a^{-1}$ であれば，$(cb)^{-1}a(cb)=a$, したがって $\{a, cb\}$ は指数2のアーベル部分群であり，同様に仮定に反する．以上により，$n=4$ の場合は完了した．

最後に $n\geqq 5$ と仮定し，P_1 を指数2の一般4元数部分群であるとする．P_1 は $a^{2^{n-2}}=1$, $b^2=a^{2^{n-3}}$, $ba=a^{-1}b$ で与えられ，$P=P_1+P_1c$ と表わされる．ここで $\{a\}$ は P_1 の位数 2^{n-2} の唯一の部分群を表わす．また，P_1 の元で $\{a\}$ に含まれないものの位数はすべて4であることに注意しよう．したがって $c^{-1}ac=a^r$ であり，$c^2=a^ib$ または $c^2=a^i$ である．もし $c^2=a^ib$ であれば $c^{-2}ac^2=a^{-1}$, したがって $r^2\equiv -1 \pmod{2^{n-2}}$ であり，これは不可能である．もし $c^2=a^i$ であれば，$\{a, c\}$ はPの指数2の部分群であり，仮定から一般4元数群である．このとき，$c^{-1}ac=a^{-1}$, $(cb)^{-1}a(cb)=a$ であり，$\{cb, a\}$ は指数2の可換部分群となり，仮定に反する．以上により定理の証明は完成した．

定理 12.5.3. 位数 p^n の p 群Pが位数 p^m（ここで $1<m<n$ とする）の部分群をただ一つだけ持つならば，Pは巡回群である．

証：まず，$m=n-1$ の場合を考える．Pが位数 p^{n-1} の唯一の部分群 P_1 を持つならば，Pは P_1 に含まれない任意の1つの元 x によって生成される．なぜならば，$\{x\}$ は唯一の極大部分群 P_1 に含まれないからである．したがって $\{x\}=P$ であり，Pは巡回群である．したがって $m=3$（定理が意味を持つ最小の n の値）の場合と，すべての n に対して $m=n-1$ なる場合に関しては，定理の証明は完成した．次に n に関する帰納法を用いて定理を証明しよう．$m=n-1$ のときは終ったから，$m<n-1$ であると仮定してよい．

P_1 を位数 p^m の唯一の部分群とし，P_1 は位数 p^{n-1} の極大部分群 A に含まれているとする．$1<m<n-1$ だから，帰納法の仮定により，A は巡回群である．したがって P_1 も A の部分群だから巡回群である．さて，位数 p または p^2 の任意の部分群は，$m\geq 2$ だからある位数 p^m の群，したがって P_1 に含まれる．しかし P_1 は巡回群だから，位数 p, p^2 の群はそれぞれただ一つしか持てない．したがって定理 12.5.2 により，P は巡回群または一般 4 元数群でなければならない．ところが，一般 4 元数群は位数 4 の部分群を 2 つ以上含む．したがって P は巡回群でなければならない．証終．

さて，アーベル群のすべての部分群が正規であることは当然である．一方，4 元数群は，すべての部分群が正規である非アーベル群である．そこで，群 H が **Hamilton 群**であるとは，H が非アーベル群であり，かつ H のすべての部分群が正規であることと定義する．このとき次の定理が成り立つ．

定理 12.5.4. Hamilton 群 H は，4 元数群，すべての元が有限奇数位数を持つアーベル群，およびすべての元の位数が 2 であるアーベル群の直積として表わされる．

証：a, b を Hamilton 群 H の 2 元とする．$\{a\}, \{b\}$ は共に正規部分群だから，交換子 $c=(a, b)=(a^{-1}b^{-1}a)b=b^s=a^{-1}(b^{-1}ab)=a^r$ が成り立つ．よって c は，a および b のいずれとも交換可能である．いま，(10.2.1) により，

$$(a^2, b)=(a, b)(a, b, a)(a, b)=(a, b)(c, a)(a, b)=(a, b)^2$$

が成り立つ．さらに，帰納法により，$(a^i, b)=(a, b)^i=c^i$ が得られる．もし a, b が交換可能でなければ $c=a^r\neq 1$ であり，このとき $i=r$ または $i=-r$ のうち正の方を選べば (a^i, b) は (c, b) または (c^{-1}, b) のいずれかである．しかし c は b と可換だから，(a^i, b) はいずれにしろ単位元である．したがって $(a^i, b)=1=(a, b)^i=c^i$ である．したがって $c^i=1, a^{ri}=1, b^{si}=1$ であり，H の交換可能でない 2 元はいずれも有限位数を持つ．もし H の元 x が a, b と共に可換であれば xa は b と可換でないから，xa したがって x は有限位数を持つ．したがって H のすべての元は有限位数を持つ．

次に，H の可換でない2元 a, b に対して，N, M を $a^N=1, b^M=1$ でかつ M, N が極小となるように選ぶ．p が N を割る素数であれば，N の極小性により a^p と b は可換であり，したがって $(a^p, b)=(a, b)^p=1$ である．M を割る任意の素数 q に対しても，同様に $(a, b^q)=(a, b)^q=1$ が成り立つ．いま，$c=(a, b)\neq 1$ だから，M と N を共に割る素数はただ一つであり，したがって $M=p^m$, $N=p^n$ と表わされる．したがって $a^{p^n}=1$, $b^{p^m}=1$, $c=(a, b)$, $c^p=1$ と表わされるが，n と m の間の対称性を考えて，$n\geq m$ と仮定してよい．さらに，$c\in\{a\}$ かつ $c\in\{b\}$ だから，$c=a^{jp^{n-1}}=b^{kp^{m-1}}$ と表わされる．ここで $j, k\not\equiv 0 \pmod p$ とする．

さて，$\{a, b\}$ の交換子群は $\{c\}$ であり，これは $\{a, b\}$ の中心に含まれることに注意しよう．したがって $\{a, b\}$ において，重さが3またはそれ以上の交換子はすべて単位元である．次に，公式

$$(ab)^i=a^ib^i(b, a)^{i(i-1)/2}$$

が成り立つことを帰納法を用いて証明しよう．$i=1$ に対しては，これは明らかである．さらに，

$$\begin{aligned}(ab)^{i+1}&=(ab)^iab\\&=a^ib^i(b, a)^{i(i-1)/2}ab\\&=a^ib^iab(b, a)^{i(i-1)/2}\\&=a^iab^i(b^i, a)b(b, a)^{i(i-1)/2}\\&=a^{i+1}b^i(b, a)^ib(b, a)^{i(i-1)/2}\\&=a^{i+1}b^{i+1}(b, a)^{i(i+2)/2}\end{aligned}$$

が成り立つ．したがって帰納法により，この公式は，(a, b) がその中心に属するような任意の群 $\{a, b\}$ に対して証明された．なお，この公式は集中公式を用いることによっても得られる．

もし $b_1=a^ub^k$（ここで $u=-jp^{n-m}$）であれば，$\{a, b_1\}=\{a, b\}$ が成り立つ．したがって b_1 は a と可換でなく，したがって仮定により，b_1 の位数は b の位数より小さくない．したがってすぐ前で得られた公式により，

$$b_1{}^p=(a^ub^k)^p$$

$$=a^{up}b^{kp}(b^k, a^u)^{p(p-1)/2}$$
$$=a^{up}b^{kp}c^{-ukp(p-1)/2}$$

が成り立つ．したがって，

$$b_1{}^{p^{m-1}}=a^{-jp^{n-1}}b^{kp^{m-1}}c^{jkp^{n-1}(p-1)/2}$$
$$=c^{jkp^{n-1}(p-1)/2}$$

である．このとき，$b_1{}^{p^{m-1}}\neq 1$ であるが，$c^p=1$ だから，$p=2$, $n=2$ でなければならない．したがって a と b の間の関係は $a^2=b^2=a^{-1}b^{-1}ab=c$, $c^2=1$ であり，$\{a, b\}$ は4元数群である．このことから分かるように，Hの非アーベル部分群は4元数群を含む．

次に，Hは，$a^4=b^4=1$, $a^2=b^2$, $ba=a^{-1}b$ で与えられた4元数群Qと，Qの各元と可換になるような元全体の作る群Zの結びとして表わされる．いま，Hの元xがaと可換でなければ，$x^{-1}ax=a^{-1}$ であり，xb はaと可換になる．同様に，もしx（または xb）がbと可換でなければ，xa（または xba）はaと可換である．したがって x, xb, xa, xba のうちの少なくとも1つはZに属する．したがって $H=Q\cup Z=QZ$ である．次に，Zは位数4の元を含まないことを示そう．もし，$x^4=1$, $x\in Z$ であれば，$(a, bx)\neq 1$ である．$(bx)^4=1$ だから，$a^{-1}(bx)a=(bx)^{-1}$ であり，したがって $a^{-1}bax=b^{-1}x^{-1}$，よって $x^2=1$ である．さて，Zは位数4の元を含まないから，Zは4元数群を含まない．したがってZはアーベル群である．また，明らかに $Z\cap Q=a^2$ である．次に，Zorn の補題により，a^2 を含まないという性質に関して極大な，Zの部分群 Z_1 を選ぶことができる．したがって直ちにわかるように，$Z=Z_1+Z_1a^2$, $H=Q\times Z_1$ が成り立つ．このとき，Z_1 は位数4の元を含まないアーベル群だから，各元の位数が奇数のアーベル群Uと，各元の位数が2のアーベル群Vの直積になっている．したがって $H=Q\times U\times V$ である．

逆に，$Q\times U\times V$ という形をした群は，Hamilton 群であることを示そう．それには，各巡回部分群 $\{quv\}$ が正規部分群であることをいえばよい．U, V は $Q\times U\times V$ の中心に属するから，a, b が $\{quv\}$ をそれ自身に変換することを示しさえすればよい．いま，$a^{-1}(quv)a=q^iuv$（$i=1$ または3）であるとす

る．u の位数は奇数 n であり，v の位数は 2 である．したがって $r\equiv i \pmod 4$, $r\equiv 1 \pmod n$ は解を持つ．したがって $a^{-1}(quv)a=(quv)^r$ である．証終．

第13章　可換群の理論

13.1. 加法群．1を法とした群

群演算は加法の形に書くこともできる．可換群は加法的に書く習慣があり，特にいくつかの演算が定義されているときに便利である．また，ある種の群はよく知られた代数系の加法から自然に生じる．特に有理数のつくる加法群を r_+，実数のつくる加法群を R_+ と書くことにする．

群を加法的に書くときは，元の和，カルテジアン和，直和といったように，積の代りに和という言葉を使うことにする．

加法的にいうと，巡回群というのは生成元 a の整数倍 na の全体になっている．r_+, R_+ においては $na=0$ ならば $a=0$ が成り立つから，これらは非周期群である． a で生成される無限巡回群においては $2x=a$ となる x は存在しない． ところが r_+ においては，任意の元 a に対して $2x=a$ となる x が存在するから，r_+ は巡回群ではない． しかし，r_+ は極めて巡回群に似た性質を持っている． すなわち，r_+ の任意の有限個の元は巡回群を生成する． この性質のことを r_+ は**階数**（rank）が1である，または**局所巡回的**（locally cyclic）であるという．もっと一般に，有限個の元で生成される部分群はすべてたかだか k 個の元で生成され，ある有限生成部分群は k 個の生成元が必要であるような可換群は，階数が k であるという．

定理 13.1.1. 有理数のつくる加法群 r_+ は局所巡回群である．

証：有限個の元 $a_1/b_1, \cdots, a_t/b_t$ で生成される r_+ の部分群を考えよう．この部分群の元は，m_i を任意の整数として，$m_1a_1/b_1+\cdots+m_ta_t/b_t$ という形をした数である．これは

$$(m_1a_1b_2\cdots b_t+\cdots+m_ta_tb_1\cdots b_{t-1})/b_1b_2\cdots b_t$$

とも書ける．この分子の全体は整数全体のつくる加法群の部分群，したがって巡回群であって，ある整数wの整数倍の全体となっている．したがって最初に考えた部分群は$nw/b_1b_2\cdots b_t$という形をした数の全体であり，巡回群となる．

群R_+の中で整数の全体は部分群をつくっているが，可換群の部分群であるから正規部分群である．したがって商群が考えられるが，そこでは差が整数となっているような数は同一視される．この商群のことを1を法とした実数群R_+とよび，$R_+ (\mathrm{mod}\ 1)$と書くことにする．同様にr_+の商群$r_+ (\mathrm{mod}\ 1)$もつくることができ，それは$R_+ (\mathrm{mod}\ 1)$の部分群になっている．

任意の有理数a/b (a, bは整数) に対し，$b(a/b)\equiv 0 (\mathrm{mod}\ 1)$となるから，$r_+ (\mathrm{mod}\ 1)$は周期群である．したがって定理3.2.3により$r_+ (\mathrm{mod}\ 1)$はそのSylow 部分群$S(p)$の直和となる．$r_+ (\mathrm{mod}\ 1)$のSylow 部分群$S(p)$のことを$Z(p^\infty)$と書くことにすると，$Z(p^\infty)$は無限集合$1/p, 1/p^2, \cdots, 1/p^i, \cdots (\mathrm{mod}\ 1)$で生成される．$Z(p^\infty)$の元は$m/p^n, (m, p)=1$という形をしていて，この元が生成する巡回群は$1/p^n$の生成する巡回群である．したがって$Z(p^\infty)$の部分群は有限群であるか，$1/p, 1/p^2, \cdots, 1/p^i, \cdots (\mathrm{mod}\ 1)$のうち無限に多くのものを含み，したがって$Z(p^\infty)$全体となる．ゆえに$Z(p^\infty)$は無限群であって，その真部分群はすべて有限巡回群である．

13.2. 可換群の指標と双対性

可換群Aが与えられているとする．Aの指標χというのは，Aから$R_+ (\mathrm{mod}\ 1)$への準同型のことである．すなわち任意の$a_1, a_2 \in A$に対し，

$$\chi(a_1)+\chi(a_2)=\chi(a_1+a_2) \tag{13.2.1}$$

を満たす．ここで，a_1+a_2というのはAでの和，$\chi(a_1)+\chi(a_2)$というのは$R_+ (\mathrm{mod}\ 1)$での和である．次に，指標の和を定義しよう．χ_1, χ_2をAの指標とするとき，$a\in A$に対し，

$$\chi_3(a)=\chi_1(a)+\chi_2(a) \tag{13.2.2}$$

と定義すると，

$$\chi_3(a_1+a_2)=\chi_1(a_1+a_2)+\chi_2(a_1+a_2) \tag{13.2.3}$$
$$=\chi_1(a_1)+\chi_1(a_2)+\chi_2(a_1)+\chi_2(a_2)$$
$$=\chi_1(a_1)+\chi_2(a_1)+\chi_1(a_2)+\chi_2(a_2)$$
$$=\chi_3(a_1)+\chi_3(a_2)$$

となるから，χ_3 もAの指標となる．(13.2.2) により指標 χ_1, χ_2 の和

$$\chi_3=\chi_1+\chi_2 \tag{13.2.4}$$

を定義すると，この和に関し指標の全体も加法群 A^* をつくる．Aのすべての元を0に写す指標が A^* の零元（単位元）である．

定理 13.2.1. 有限可換群Aの指標群 A^* はAと同型である．

証：χ をAの指標とすると，χ はAから $R_+(\mathrm{mod}\,1)$ への準同型であるから，$\chi(0)=0$ でなければならない．そこでAの元 a の位数がmだとすると，$m\chi(a)=\chi(ma)=x(0)=0$ となる．したがって，$\chi(a)$ の値は $0, 1/m, \cdots, (m-1)/m$ $(\mathrm{mod}\,1)$ のm個のうちの1つでなければならない．有限可換群の指標は基底での値により完全に決まる．そこで，$a_i, i=1, \cdots, r$ をAの1つの基底とし，a_i の位数を n_i とすると，Aの位数は $n=n_1n_2\cdots n_r$ となる．$\chi(a_i)$ の選び方はたかだか n_i 通りだから，Aの異なる指標の数はたかだか $n=n_1n_2\cdots n_r$ である．一方，実際にこれだけ指標があることが容易にわかる．すなわち，各 $i=1, \cdots, r$ に対し，$\chi_i(a_i)=1/n_i, \chi_i(a_j)=0, j\neq i,$ と定義すると χ_i は指標となり，$a_i \leftrightarrows \chi_i$ という対応がAと A^* の間の同型を与える．ただし，Aと A^* の間の同型対応は，Aの基底の取り方に依存し，一意的には定まらないことに注意する．

次の定理は有限，無限を問わず，任意の可換群に対し成り立つ．

定理 13.2.2. Hを可換群Aの部分群とする．このとき，Aの指標 χ で，任意の $h\in H$ に対し $\chi(h)=0$ となるものの全体と，商群 A/H の指標の全体とは一致する．

証：H の各元に対し0を対応させる指標は剰余類 $H+x$ の各元に対し同じ値をとる．そこでこの値を商群 A/H の元 $H+x$ でとる値とみることにより，

A/H の指標を与えることが容易に分かる．逆に $A \to A/H$ の自然な準同型を A/H の指標，すなわち A/H から $R_+ \pmod 1$ への準同型と合成すると，A から $R_+ \pmod 1$ への準同型，すなわちAの指標が得られるが，これはHの各元を0に写す．

系 13.2.1. 有限可換群 A の 0 でない任意の元 a に対し，A の指標 χ で $\chi(a) \neq 0$ を満たすものが存在する．

証：これが成立しないとすると，Aの任意の指標が商群 $A/\{a\}$ の指標となるが，すると定理 13.2.1 により A^* はAにも $A/\{a\}$ にも同型となる．ところが $A/\{a\}$ の位数はAの位数よりも本当に小さいから，このようなことは起こらない．

群AとBとの間の**双対** (duality) というのは，Aの部分群HとBの部分群Kとの間の一対一対応 $H \leftrightarrows K$ で，包含関係を逆にするもののことである．すなわち，$H_1 \leftrightarrows K_1$, $H_2 \leftrightarrows K_2$ という対応があるとき，$H_1 \supset H_2$ ならば $K_1 \subset K_2$ となり，逆に $K_1 \subset K_2$ ならば $H_1 \supset H_2$ となる．有限可換群Aとその指標群 A^* との間には自然な双対のあることが次の定理で示される．

定理 13.2.3. 有限可換群 A とその指標群 A^* との間には次のような対応 $H \leftrightarrows K$ により双対が存在する．すなわち，Aの部分群Hに対しては，任意の $h \in H$ に対し $\chi(h)=0$ となる指標 χ の全体Kを対応させ，A^*の部分群Kに対しては，任意の $\chi \in K$ に対し $x(h)=0$ となるAの元 h の全体Hを対応させる．また，Aは自分自身に双対である．

証：Aの部分群Hに対し，A^* の部分群 H^* を任意の $h \in H$ に対し $\chi(h)=0$ となる指標 χ の全体と定義しよう．H_1 と H_2 を A の異なる部分群とすると，H_1 か H_2 の少なくとも一方，たとえば H_1 は他方に含まれていない元 b を含む．すると定理 13.2.2 により H_2^* は A/H_2 の指標群であり，系 13.2.1 により H_2^* は $\chi(b) \neq 0$ となる指標 χ を含む．ゆえに $H_1^* \neq H_2^*$ が成り立つ．ところがAと A^* は有限群で同型だから，$H \to H^*$ という写像はAの部分群と A^* の

部分群との間の一対一対応を与え，特に A^* の任意の部分群 K に対し $K=H^*$ となる A の部分群 H が一意的に存在する．$H_1 \leftrightarrows K_1=H_1^*$, $H_2 \leftrightarrows K_2=H_2^*$ のとき，$H_1 \supset H_2$ とすると，任意の $h \in H_1$ に対して $\chi(h)=0$ ならば，任意の $h \in H_2$ に対して $\chi(h)=0$ となるから，$K_1 \subset K_2$ が成り立つ．同様に $K_1 \subset K_2$ とすると $H_1 \supset H_2$ が成り立つ．ゆえに定理における対応は A と A^* との間の双対を与える．そして A と A^* が同型だから，A は A 自身と双対になる．

定理 13.2.4. Sylow 部分群がすべて有限群であるような周期的可換群は自分自身に双対である．

証：A を周期的可換群でその Sylow 部分群はすべて有限群だとする．すると，Sylow 部分群 $S(p)$ は自分自身に双対である．そこで，$S(p)$ の部分群 H_p に対し，その双対を $H_p{}^d$ と書くことにする．さて，H を A の任意の部分群とすると，H はその Sylow 部分群 H_p の直和となる．そこで $H^d=\sum_p H_p{}^d$ と置くと，これが A の双対を与えることが容易に分かる．ただし，単に有限可換群の直和になっているというだけでは上の議論は適用できないことに注意する．というのは，一般には直和因子の部分群の直和として表わせない部分群が存在するからである．実際，双対をもつ可換群はこの定理に述べたものに限ることが Baer [6] によって示された．

13.3. 可　除　群

加法的に書かれた可換群 A が**可除群** (divisible group) であるとは，任意の $a \in A$ と任意の自然数 n に対し $nx=a$ となる $x \in A$ が存在することと定義する．

定理 13.3.1. 可除群はそれを含む任意の可換群の直和因子になる．

証：可換群 A とその可除部分群 D が与えられたとする．このとき

(13.3.1)　　$A=D \oplus B$, すなわち，$D \cap B=0$, $D \cup B=A$

となる部分群 B が存在することを証明しよう．それには §1.8 で論じた Zorn の

補題を使うのが便利である．$U_1 \subset U_2 \subset U_3 \subset \cdots$ を $D \cap U_i = 0$ を満たすAの部分群の昇鎖とすると，$U = \bigcup_i U_i$ も $D \cap U = 0$ という性質を満たす．よって Zorn の補題により，$K \cap D = 0$ という性質を満たすAの部分群の中で極大なものKが存在する．$D \cup K = A$ を示せば，(13.3.1) のBとしてこのKをとることができる．いまAのある元xが $K \cup D$ に入らなかったとすると，Kの極大性により，$\{x\} \cup K$ とDとの共通部分は0でない元を含む．ゆえに適当な非負整数nと $k \in K$ により，$nx + k = d \in D, d \neq 0$ とできる．$D \cap K = 0$ だからnは0ではない．$n = 1$ とすると $x \in K \cup D$ となり仮定に反する．Dは可除群であるから，$d = nd_1$ となる $d_1 \in D$ が存在し，$n(x - d_1) = -k$ となる．そこで $x_1 = x - d_1$ と置く．$x_1 \in K \cup D$ とすると，$x \in K \cup D$ となり，仮定に反する．$K \cup \{x_1\}$ の元は $mx_1 + k$, $0 \leq m < n$ という形に書ける．Kの極大性より $\{x_1\} \cup K$ とDの共通部分に0でない元dが存在して，$n_1x_1 + k_1 = d = n_1d_2$, $n_1 < n$, d, $d_2 \in D$ と書ける．そこで $x_2 = x_1 - d_2$ と置くと，$n_1x_2 = -k_1 \in K$ となる．もし $x_2 \in K \cup D$ とすると，$x_1 \in K \cup D$ となるから，$x_2 \notin K \cup D$ でなければならない．これを繰り返していくと，最後には $n_i = 1$ となり，$x_i, x_{i-1}, \cdots, x_1$ そしてxがすべて $K \cup D$ に属すことになり，仮定に反する．ゆえに $K \cup D = A$ となり，定理が証明された．

任意の可除群は r_+ または $Z(p^\infty)$ に同型な群の直和になる．証明は Kaplansky [1] を見られたい．

13.4. 純部分群

Hが可換群Aの純部分群であるとは，ある $x \in A$ に対して $nx = h \in H$ となったとすると，$nh_1 = h$ となる $h_1 \in H$ が存在することと定義する．つまり，純部分群であるという性質は一種の相対的可除性であり，除算ができるときはHの中でできるということである．明らかに可除群はそれを含む任意の可換群の純部分群である．また直和因子は純部分群になる．可除群は必ず無限群だが，有限群にも純部分群が存在するから，純部分群というのは有限群の研究においても有用な概念である．

可換群の周期部分群[1]は純部分群である．なぜなら，$nx=h$ で h が位数有限とすると，x も位数有限となるからである．また純部分群の昇鎖の結びも純部分群である．なぜなら，h をこの結びの元とすると，h はこの昇鎖の中のどれかの部分群に入り，$nx=h$ というのは，解があるならばその部分群の中に解があり，この昇鎖の結びの中に解を持つからである．

直和因子は純部分群になるが，逆に次の定理 13.4.1 は純部分群が多くの場合直和因子になることを示している．

定理 13.4.1. H を可換群 A の純部分群とし，A/H が巡回群の直和になったとすると，H は A の直和因子となる．

証：まず次の補題を証明する．

補題 13.4.1. H を A の純部分群，y を A/H の元とすると，$A \to A/H$ の準同型により y に写される A の元 x で，y と同じ位数のものが存在する．

y の位数が無限ならば，y に写される A の任意の元 x も位数無限である．$ny=0$ で $u \to y$ とすると，$nu \to 0$ であるから，$nu=h \in H$ となる．H が純部分群だから $h=nh_1$ となる $h_1 \in H$ が存在する．そこで $x=u-h_1$ と置けば，$x \to y$ で $nx=n(u-h_1)=nu-nh_1=0$ となり補題が証明された．

この補題を使えば，定理の証明はかなり簡単になる．A/H が基底元 $y_i, i \in I$ で生成される巡回群の直和とする．上の補題により，$x_i \to y_i$ で x_i が y_i と同じ位数になるように $x_i \in A$ が選べる．K を x_i で生成される部分群とする．もし $n_{i_1}x_{i_1}+\cdots+n_{i_s}x_{i_s}=h \in H$ となったとすると，A/H においては $n_{i_1}y_{i_1}+\cdots+n_{i_s}y_{i_s}=0$ となるが，$\{y_i\}$ は A/H の基底だったから，各項とも $n_i y_i=0$ となる．ところが x_i は y_i と同じ位数だったから，各項とも $n_i x_i=0$ となり h は 0 となる．ゆえに $K \cap H=0$ である．また K は A の各剰余類の元を 1 つずつ含んでいるから $K \cup H=A$ となる．ゆえに $A=H \oplus K$ となり，定理が証明された．

---

[1] 位数有限の元の全体がつくる部分群．

13.5. 一般的注意

可換群のもっと詳しい研究については，Kaplansky の論文［1］，Kurosch の本［2］の第II部を見られたい．特に Kaplansky の論文で文献について論じている部分は有用である．

一般に定理 3.2.3 により周期群の研究は準素群[1)]の研究に帰着される．準素群に関する主要な結果の1つは Ulm の定理である．それは可算濃度の準素群を"Ulm の不変数列"とよばれるある種の濃度により，完全に特徴づけるものである．

無限巡回群の直和は**自由可換群**（free Abelian group）とよばれる．r 個の生成元をもつ可換群は r 個の生成元をもつ自由可換群の準同型像となる．巡回群の直和の部分群はそれ自身巡回群の直和となり，特に自由可換群の部分群は自由可換群である．

§13.3 で注意したように，任意の可除群は r_+ または $Z(p^\infty)$ に同型な群の直和となる．任意の可換群は可除群の中に埋め込むことができ，したがって可換群の研究は，ある意味では可除群の部分群の研究ということもできる．特に階数1の非周期群は r_+ の部分群である．

位数有限の元も，無限の元も含んでいる可換群は**混合群**（mixed group）とよばれる．一般には混合群を周期部分群と非周期群の直和として表わせない例が存在する．しかし，周期部分群は純部分群であるから，定理 13.4.1 により，混合群が周期部分群と他の群との直和に分解されるということはしばしば起こる．

---

1) 可換 p-群のこと．

第14章　単項表現と移送

14.1. 単　項　置　換

群Hの元を左から掛けることのできる不定元 $u_1, \cdots, u_n$ の集合Sを考えることにする[1]．ただし，群の作用については，1をHの単位元とするとき，

(14.1.1) $$1u_i = u_i,$$

および

$$h_1(h_2u_i) = (h_1h_2)u_i$$

が成り立つとする．**単項置換** (monomial permutation) Mというのは，$u_i \to h_{ij}u_j, i=1, \cdots, n$ という写像のことである．ただし $j=j(i)$ で，$u_i \to u_j$ はSの置換とする．2つの写像 $M_1: u_i \to h_{ij}u_j$ および $M_2: u_j \to h'_{jk}u_k$ に対し，M_1 と M_2 の積 M_1M_2 を $u_i \to (h_{ij}h'_{jk})u_k$ で定義する．この定義により単項置換の全体は群をつくり，$u_i \to u_i$ という写像が単位元となる．写像 $M_1: u_i \to h_{ij}u_j$ に対し，i 行 j 列要素が h_{ij} で他の要素は0である行列 (h_{ij}) を対応させると，上で定義した写像の積は普通の行列の積と一致する．

単項置換全体のつくる群Mの中で，$u_i \to h_{ii}u_i$ という写像の全体は正規部分群Dをつくり，商群 M/D は $u_1, \cdots, u_n$ の置換全体のつくる対称群になる．もっと一般に，GをMの部分群とし，$g \in G$ が $u_i \to h_{ij}u_j$ のとき，g^* を $u_i \to u_j$ と定義すると，$g \to g^*$ はGからある置換群の上への準同型でその核は $G \cap D$ となる．

単項置換群Gは，対応する置換群が可移的であるとき，可移的であるとよぶことにする．

---

1) $hu_i (h \in H, u_i \in S)$ という記号の全体Aの上にHが作用していると考える．また (14.1.1) によりSはAの中に埋め込まれているとみなされる．

定理 14.1. Kを群Gの部分群で，$G=K+Kx_2+\cdots+Kx_n$ とする．そして $K\to H$ をKからある群Hの上への準同型とすると，Hを作用群とするGの可移単項表現が次のようにして得られる：$g\in G$ について $x_ig=k_{ij}x_j,\ i=1,\cdots,n,\ j=j(i),\ k_{ij}\in K$ となっていたとし，準同型 $K\to H$ により $k_{ij}\to h_{ij}$ となっていたとする．このとき，$\pi(g):u_i\to h_{ij}u_j$ はHを作用群とするGの可移単項表現となる．逆に，任意の可移単項表現はDによる共役を除けばこのようにして得られる．

証：群G, 左剰余類分解 $G=K+Kx_2+\cdots+Kx_n$, および準同型 $K\to H$ が与えられたとし，g_1, g_2 をGの任意の元とする．もし $x_ig_1=k_{ij}x_j,\ x_jg_2=k'_{js}x_s$ とすると，$x_i(g_1g_2)=k_{ij}k'_{js}x_s$ となるから，対応する単項置換について $\pi(g_1g_2)=\pi(g_1)\pi(g_2)$ が成り立つ．これでGの表現が得られた（もちろん，忠実な表現とは限らない）．対応する置換群は §5.3 で論じられた左剰余類上の置換群だから，当然可移的である．

逆に，Gの任意の可移単項表現Rを考えることにしよう．ただし，$g\in G$ に対し，$R:g\to\pi(g),\ \pi(g):u_i\to h_{ij}u_j$ とする．特定の文字 u_1 を選び，Gの元kで $\pi(k)$ が u_1 を $h_{11}u_1(h_{11}\in H)$ に写すものの全体KはGの部分群をつくる．Rの可移性により，各 $i=2,\cdots,n$ に対し，$\pi(x_i)$ が u_1 を $h_{1i}u_i$ に写す様なGの元 x_i が存在する．このとき

(14.1.2)
$$G=K+Kx_2+\cdots+Kx_n$$

が成り立つことが容易にわかる．Dの元 $d:u_1\to u_1,\cdots,u_i\to h_{1i}^{-1}u_i,\cdots,u_n\to h_{1n}^{-1}u_n$ によりRを変換すると，$d^{-1}Rd$ において $d^{-1}\pi(x_i)d$ は u_1 を u_i に写す．以下，Rのかわりに $R^*=d^{-1}Rd$ を考えることにする．このとき，$k\in K$ について，$\pi(k)$ が u_1 を hu_1 に写すことと，$\pi(x_i^{-1}kx_j)$ が u_i を hu_j に写すこととは同値となる．したがって R^* においては，Gのある元に対して作用元として出てくるhは，Kの元に対して出てくる．このようなHの元の全体 H_1 は，Hの真部分群であるかもしれないが，$\pi(k)$ が u_1 を hu_1 に写すとき，$k\to h$ と定義すると，これはKから H_1 の上への準同型となる．そして，$\pi(g)$ が

u_i を $h_{ij}u_j$ に写すとき，$\pi(x_i g x_j^{-1})$ は u_1 を $h_{ij}u_1$ に写すから，$x_i g x_j^{-1}=k_{ij}$ $\in K$ となり，$K \to H_1$ の準同型により $k_{ij} \to h_{ij}$ となる．

KによるGの左剰余類の代表系をとりかえたとき得られる単項表現は，最初の表現とDにより共役となることをついでに注意しておく．

14.2. 移　　　送

Hを作用群とする群Gの単項表現 $R: g \to \pi(g)$,

(14.2.1) $$\pi(g): u_i \to h_{ij}u_j,\ i=1, \cdots, n,\ j=j(i)$$

が与えられたとする．さらに文字の数nは有限とする．このとき，Hの交換子群をH'とすると，

(14.2.2) $$g \to \prod_{i=1}^{n} h_{ij} \bmod H'$$

はGから商群 H/H' への準同型となることが容易に分かる．特に $H=K$ の場合を考える．Gの左剰余類分解を

(14.2.3) $$G=K+Kx_2+\cdots+Kx_n$$

とし，$z=kx_j, k\in K$ のとき $\phi(z)=x_j$ と置くと，上の写像は

(14.2.4) $$V_{G\to K}(g) \equiv \prod_{i=1}^{n} x_i g \phi(x_i g)^{-1} \bmod K'$$

となり，$V_{G\to K}$ はGから K/K' への準同型となる．この準同型はGからKへの**移送**（transfer, ドイツ語では Verlagerung）とよばれる．もしHがKの準同型像ならば，K'はKの全不変部分群だから，$K \to H$ により K/K' は H/H' の上に写され，(14.2.2) の写像は移送の準同型像となる．移送に関する最も重要な性質は次の定理 14.2.1 で与えられる．

定理 14.2.1.

1) 写像 $g \to V_{G\to K}(g)$ はGから K/K' への準同型である．

2) 移送 $V_{G\to K}(g)$ は代表系 x_i の選び方によらない．

3) $G\supset K\supset T$ ならば，$V_{G\to T}(g)=V_{K\to T}[V_{G\to K}(g)]$ となる．

証：単項表現の理論の結果として最初の性質が成り立つことはすでにわかっ

ているが，これら３つの性質をすべて移送の定義（14.2.4）から直接証明することにする．まず，$x_i g_1 = k_{ij} x_j,\ i=1, \cdots, n,\ x_i g_2 = k'_{js} x_s,\ j=1, \cdots, n$ とすると，$V_{G\to K}(g_1) \equiv \prod_i k_{ij} \bmod K'$，$V_{G\to K}(g_2) \equiv \prod_j k'_{js} \bmod K'$ となり，$k_{is}{}^* = k_{ij} k'_{js}$ と置くと，$V_{G\to K}(g_1 g_2) \equiv \prod_i (k_{is}{}^*)$ となることから最初の性質が出てくる．次に２つの代表系の間に $x_i{}^* = a_i x_i$ という関係が成り立っていて，$x_i g = k_{ij} x_j$ とすると，$x_i{}^* g = a_i x_i g = a_i k_{ij} x_j = a_i k_{ij} a_j{}^{-1} x_j{}^*$ となるから，$V(g)$ は一方では $\prod_i k_{ij} \bmod K'$ に等しく，もう一方でも $\prod_i (a_i k_{ij} a_j{}^{-1}) \equiv \prod_i a_i \cdot \prod_i k_{ij} \cdot \prod_j a_j{}^{-1}$ $\equiv \prod k_{ij} \bmod K'$ となることから２番目も成り立つ．３番目の性質は，

(14.2.5)
$$G = K + Kx_2 + \cdots + Kx_n,$$
$$K = T + Ty_2 + \cdots + Ty_m$$

とすると，

$$\begin{aligned} G = {} & T + Ty_2 + \cdots + Ty_m \\ & + \cdots \\ & + Tx_i + Ty_2 x_i + \cdots + Ty_m x_i \\ & + \cdots \\ & + Tx_n + Ty_2 x_n + \cdots + Ty_m x_n \end{aligned}$$

となる．そこで $g \in G$ に対し，

$$x_i g = k_{ij} x_j, \quad y_r k_{ij} = t_{ijrs} y_s$$

とすると，

$$y_r x_i g = t_{ijrs} y_s x_j$$

となるから，

$$V_{G\to T}(g) \equiv \prod_{i,r} t_{ijrs} \bmod T',$$
$$V_{G\to K}(g) \equiv \prod_i k_{ij} \bmod K'$$

となる．そして

$$V_{K\to T}(k_{ij}) \equiv \prod_r t_{ijrs} \bmod T'$$

だから

$$V_{G\to T}(g) \equiv \prod_i V_{K\to T}(k_{ij}) \bmod T'$$

$$\equiv V_{K\to T}(\prod_i k_{ij}) \bmod T'$$
$$\equiv V_{K\to T}[V_{G\to T}(g)]$$

となる．ここで $V_{G\to K}(g)$ はKの元ではなく，K/K' の元であるが，KからTへの移送は K' を単位元に写すから，$V_{G\to K}(g)$ のTへの移送にあいまいさは残らないことを注意しておく．

14.3. Burnside の定理

定理 14.3.1. 有限群Gの Sylow 部分群PがPの正規化群の中心に入っていれば，Gの正規部分群Hで，その剰余類の代表系としてPの元の全体を取ることができるようなものが存在する．

証：まず次の補題を証明する．

補題 14.3.1. もし2つの複体 K_1, K_2 がGの Sylow 部分群Pの中で正規で，Gにおいて共役ならば，K_1 と K_2 は $N_G(P)$ において共役である．

補題の証：$x^{-1}K_1x=K_2, x\in G$ とする．K_1 は P において正規だから，$K_2=x^{-1}K_1x$ は $x^{-1}Px=Q$ において正規である．したがって，P, Q は共に K_2 の正規化群の中に入り，$N_G(K_2)$ の Sylow 部分群である．したがって $N_G(K_2)$ の中で共役となり，$y^{-1}K_2y=K_2$ を満たすある y により $y^{-1}Qy=P$ となる．そこで $z=xy$ と置くと，$z^{-1}Pz=P$, $z^{-1}K_1z=K_2$ となり，補題が証明された．

定理の証明は，Pが $N_G(P)$ の中心に入るから，Pは可換群で，$P'=1$ となる．そこで$V_{G\to P}$を考えることにする．$u\in P$ とし，$V_{G\to P}(u)$ を計算するのに，PのGにおける代表系として $x_i, x_iu, \cdots, x_iu^{r-1}$ を使うことにする．ただし，$j<r$ ならば，$x_iu^j \notin Px_i$, $x_iu^r\in Px_i$ とする．$j<r$ ならば，$x_iu^{j-1}\cdot u\cdot\phi(x_iu^j)^{-1}=x_iu^ju^{-j}x_i^{-1}=1$ で，$x_iu^{r-1}\cdot u\cdot\phi(x_iu_r)^{-1}=x_iu^rx_i^{-1}$ となる．したがって，uをPによる左剰余類上に表現したときの長さ r の各巡環に対し，$V_{G\to P}(u)$ を表わす積の中に $x_iu^rx_i^{-1}$ という項が1つずつあり，残りは単位元である．よって

$V_{G\to P}(u)=\prod_i x_i u^r x_i^{-1}$ となる．さて，$x_i u^r x_i^{-1}\in P$ はGにおいて u^r に共役となり，Pは可換群だから，この２つの元はPにおいて正規である．したがって上の補題により，適当な $y\in N_G(P)$ により，$x_i u^r x_i^{-1}=y^{-1}u^r y$ となるが，P がその正規化群の中心に入るという仮定により $y^{-1}u^r y=u^r$ となる．ゆえに $V_{G\to P}(u)\equiv \prod u^r\equiv u^n$ となる．ただし $n=[G:P]$ はすべての巡環の長さの和である．Pは Sylow 部分群であるから，たとえば位数を p^s とすると，p は $n=[G:P]$ を割らない．したがってGのPへの移送において，Pは自分自身の上へ同型に写され，$V_{G\to P}(G)=P$ となる．この準同型の核はGの指数 p^s，したがって位数 $n=[G:P]$ の正規部分群Hで，Pの元の全体がHによる剰余類の代表系として取ることができる．

系 14.3.1. 有限単純群の位数は 12，またはその位数を割る最小の素数の３乗で割り切れる．

証：単純群Gの位数を割る最小の素数をpとする．Gの Sylow p-部分群Pの位数がpまたは p^2 だったとすると，Pは可換群となる．$N_G(P)$ がPに自明でない自己同型を引き起こさなければ，上の定理により，GはPを商群として持ち，単純にならない．もしPの位数がpならば，Pの自己同型群の位数は $p-1$ でpより小さい．またPの位数が p^2 のときのPの自己同型群の位数は，Pが巡回群のときは $p(p-1)$ で，Pが巡回群でないときは $(p^2-1)(p^2-p)=p(p-1)^2(p+1)$ である．もしpが奇数ならば，$p+1=2[(p+1)/2]$ だから，自己同型群の位数はpより大きな素数では割り切れず，$N_G(P)$ によって自明でない自己同型は引き起こされない．$p=2$ ならば，最後の場合において，$p+1=3$ となり，$N_G(P)$ がPに位数３の自己同型を引き起こすことが可能だが，それは $N_G(P)$ の位数が 12 で割り切れるときだけである．

14.4. P. Hall, Grün および Wielandt の定理

この節の定理は，群Gの Sylow p-部分群とGの商群 G/K で p-群となるものとの間の関係が主要内容である．

この関係を記述するために，強い意味および弱い意味で閉じているという概念を導入する．

定義：Gの部分群HとHの部分群Bについて，任意の $x\in G$ に対し，$H\cap B^x\subseteq B$（ただし $B^x=x^{-1}Bx$）が成り立つとき，BはHにおいて（Gに関し）強い意味で閉じている（strongly closed）といい，$B^x\subseteq H$ ならば $B^x=B$ が成り立つとき弱い意味で閉じている（weakly closed）という．

群Gのある Sylow p-部分群Pの中心Zが，それを含む任意の Sylow p-部分群 P_1 の中心になっているとき，群Gは **p-正規**（p-normal）であるという．これは弱い意味で閉じているということの特別な場合になっている．つまり，Pの中心ZがPにおいてGに関し弱い意味で閉じているということと同値である．なぜなら，Gが p-正規とし，$Z^x\subseteq P$, $x\in G$ とすると，Zは $P_1=P^{x^{-1}}$ に含まれる．したがって，Gの p-正規性によりZは P_1 の中心になる．すると，Z^x は $P_1{}^x=P$ の中心になるから $Z^x=Z$ となり，ZはPにおいて弱い意味で閉じている．逆にZがPにおいて弱い意味で閉じているとし，別の Sylow 部分群 P_1 が Z を含んでいるとする．すると，ある $x\in G$ により $P_1{}^x=P$ となり，このxにより $Z^x\subseteq P$ となるが，弱い意味で閉じていることから $Z=Z^x$ となる．ところが，P_1 の中心を Z_1 とすると $Z_1{}^x$ は $P_1{}^x=P$ の中心であるから，$Z_1{}^x=Z=Z^x$ となり，$Z=Z_1$ は P_1 の中心である．ゆえにGは p-正規となることが分かった．

強い意味で閉じていれば，明らかに弱い意味でも閉じている．またHにおいて弱い意味で閉じている部分群BはHの正規部分群でなければならない．方程式 $x^k=1$ を満たすすべてのxで生成されるHの部分群は弱い意味で閉じており，もしこのようなxが部分群Xをつくっているならば，XはHにおいて強い意味で閉じている．Hが正則 p-群のときなどにこのようなことが起こっている．

以下，誤解が起こらないときは，移送 $V_{G\to H}(g)$ のことを $V(g)$ と書くことにする．したがって，もし

$$G=H+Hx_2+\cdots Hx_m$$

ならば，

$$V(g)\equiv\prod_{i=1}^{n}x_i g\phi(x_i g)^{-1}\ \mathrm{mod}\ H'$$

となる．また H' を含む H の任意の部分群 H_0 をとると，H/H_0 は可換群であるから，H' を法としての合同を考えるかわりに，H_0 を法として考えてもよい．以下では H_0 を法として考えることにする．

$g\in G$ と $i=1,\cdots,n$ に対し，ig を $1,\cdots,n$ の中で，$x_i g x_{ig}{}^{-1}\in H$ となるものと定義する．すると，固定した g に対し，$i\to ig$ は，H による左剰余類上の G の可移置換表現の置換 $\pi(g)$ である．したがって

$$V(g)\equiv\prod_i x_i g x_{ig}{}^{-1}$$

と書くことができる．置換 $\pi(g)$ には，固定する文字も長さ1の巡環とみなして，いくつかの巡環があるが，各巡環から1つずつ代表を選び，この集合を $C_H(g)$ と書くことにする．$i\in C_H(g)$ に対し，r_i を i が現われる巡環の長さとすると，

$$\sum_{i\in C_H(g)}r_i=n$$

となるが，これは巡環の長さの総計が n であることを意味している。

補題 14.4.1. $$V(g)\equiv\prod_{i\in C_H(g)}x_i g^{r_i} x_i^{-1}.$$

ただし $x_i g^{r_i} x_i^{-1}$ は $x_i g x_i^{-1}$ の巾の中で，はじめて H に入るものである。

証：i からはじまる $\pi(g)$ の巡環の中で，$i, ig, \cdots, ig^{r_i-1}$ はすべて異なっているから，$x_i, x_i g, \cdots, x_i g^{r_i-1}$ を対応する H の剰余類の代表にとることができる．$\phi(x_i g^s)=x_i g^s$, $s=1,\cdots,r_i-1$, $\phi(x_i g^{r_i})=x_i$ であるから，これらの剰余類は $V(g)$ に

$$x_i g(x_i g)^{-1}\cdot(x_i g)g(x_i g^2)^{-1}\cdot(\cdots)\cdot(x_i g^{r_i-1})g x_i^{-1}=x_i g^{r_i} x_i^{-1}$$

だけ帰与する．$s<r_i$ に対しては，$x_i g^s\notin Hx_i$ だから，$x_i g^{r_i} x_i^{-1}$ は $x_i g x_i^{-1}$ の巾の中ではじめて H に入るものである．

$V(g)$ のうち長さ1の巡環から出てくるものを**対角成分** (diagonal contribution) $d(g)$ とよぶことにすると，

$$d(g)\equiv\prod_{i=ig} x_i g x_i^{-1} \bmod H_0$$

と書かれる．このとき，$V(g)$ と同様に $d(g)$ も H_0 を法として考えれば，成分のならべ方や代表系 x_i の選び方には関係しない．

補題 14.4.2. u, v が G において共役ならば $d(u)\equiv d(v)$ となる．また $d(u^{-1})\equiv[d(u)]^{-1}$ が成り立つ．

証：$v=t^{-1}ut$ とすると $iu=i$ ということと，$itv=it$ ということとは同値となる．したがって対角成分の定義と $x_{it}t^{-1}x_i^{-1}, x_i t x_{it}^{-1}$ が共に H の元で，互いに逆元であることから

$$\begin{aligned} d(v)&\equiv\prod_{i=iu} x_{it} v x_{it}^{-1} \\ &\equiv\prod_{i=iu} (x_{it}t^{-1}x_i^{-1})(x_i u x_i^{-1})(x_i t x_{it}^{-1}) \\ &\equiv\prod_{i=iu} (x_i u x_i^{-1}) \\ &\equiv d(u) \end{aligned}$$

となる．また $i=iu$ ということと，$i=iu^{-1}$ ということとは同値だから

$$\begin{aligned} d(u^{-1})&\equiv\prod_{i=iu} x_i u^{-1} x_i^{-1} \\ &\equiv(\prod_{i=iu} x_i u x_i^{-1})^{-1} \\ &\equiv[d(u)]^{-1} \end{aligned}$$

となることが分かる．

$h\in H$ に対し，$d^*(h)\equiv h^{-1}d(h)$ と定義する．すると補題 14.4.2 より $h\equiv d(h)[d^*(h)]^{-1}\equiv d(h)d^*(h^{-1})$ となり，また同じく補題 14.4.2 より $d(h^r)\equiv d(x_i h^r x_i^{-1})$ となるから，$x_i h^r x_i^{-1}\in H$ ならば

$$\begin{aligned} x_i h^r x_i^{-1}&\equiv d(h^r)d^*(x_i h^{-1} x_i^{-1}) \\ &\equiv h^r d^*(h^r)d^*(x_i h^{-r} x_i^{-1}) \end{aligned}$$

となり，最後に補題 14.4.1 より

補題 14.4.3. $h\in H$ ならば

$$V(h)\equiv h^n \prod_{i\in C_H(h)} d^*(h^{r_i})d^*(x_i h^{-r_i} x_i^{-1})$$

となる．

系 14.4.1. もしすべての $h\in H$ に対して，$d^*(h)\in H_0$ が成り立つならば，任意の $h\in H$ に対し，$V(h)\equiv h^n$ となる．

pを1つの素数，G_1 を任意の有限群とし，$G=u_p(G_1)$ を位数が p と素な G_1 の元全体で生成された部分群とする．したがって G_1/G はGの極大 p–商群である．P_1 を G_1 の Sylow p–部分群，その G_1 における正規化群を N_1 とし，H_1 を N_1 を含む G_1 の任意の部分群とする．$P=P_1\cap G$, $N=N_1\cap G$, $H=H_1\cap G$ と置くと，$G_1=GP_1=GN_1=GH_1$ となり，$P_1/P=N_1/N=H_1/H=G_1/G$ が成り立つ．Gは G_1 の全不変部分群で，PはGの Sylow p–部分群となり，Nは P_1 および G, したがって $P_1\cap G=P$ を正規化することを注意しておく．Gは位数がpと素な元で生成されているから $u_p(G)=G$ であるが，$u_p(H)\subset H$ ということは起こり得る．そこで，以下 $u_p(H)\subset H$ と仮定しよう．$u_p(H)$ はHの全不変部分群でHは H_1 の正規部分群である．実際 H_1/H は p–群だから明らかに $u_p(H)=u_p(H_1)$ となる．そこで

$$H_0=H^p\cup(H,H_1)\cup u_p(H)$$
$$=H^p(H,H_1)u_p(H)$$

と定義する．ここで H^p というのはHの元のp乗で生成された群で，(H,H_1) というのは交換子 (h,h_1), $h\in H$, $h_1\in H_1$ で生成された群のことである．$H_1/u_p(H)$ は p–群で，これらの3つの群は特性部分群だから，これらの結び は積になる．また $u_p(H)=u_p(H_1)$ であるから，$H_1/u_p(H)$ は p–群，したがって巾零になる．よって $(H,H_1)/u_p(H)$ は $H/u_p(H)$ の真部分群である．さらに，$H\supset T\supset(H,H_1)u_p(H)$ で $[H:T]=p$

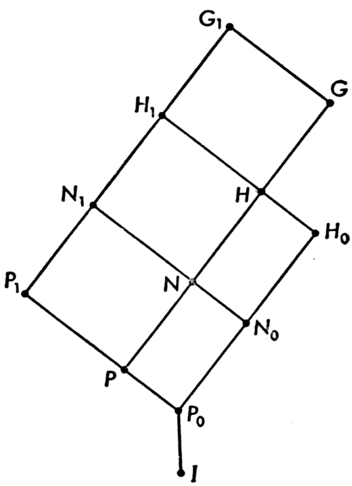


図 6. Philip Hall の定理

を満たす任意の部分群 T に H^p が含まれるから，$u_p(H)$ が H の真部分群ならば H_0 も H の真正規部分群で，H/H_0 は p-群となる．次の問題を考えてみよう：Hを生成するためには H_0 にPのどのような元をつけ加えなければならないか？

補題 14.4.4. H は H_0 とすべての $u\in P$ に対する $d^*(u)$ の全体とで生成される．

証：ここでも前と同じく

$$G=H+Hx_2+\cdots+Hx_n,$$
$$d(u)\equiv\prod_{i=iu}x_iux_i^{-1}\bmod H_0,$$
$$d^*(u)\equiv u^{-1}d(u)\bmod H_0$$

とする．H_0 の選び方から，$H_0\supseteq(H,H_1)\supseteq(H,H)=H'$ だから，確かに H/H_0 は可換群になっていることに注意する．$u\in P\subseteq H$ だから，$d^*(u)\in H$ は確かに成り立っている．したがって $K=\{d^*(u)|u\in p\}\cup H_0\subseteq H$ である．$H\subseteq K$ を証明するためには，H/H_0 は可換 p-群だから，位数が p と素な G の元 w に対しては $V(w)\equiv 1(\bmod H_0)$ となるが，G のつくり方から，G はこのような元で生成されており，任意の $u\in G$ に対し，$V(u)\equiv 1(\bmod H_0)$ となる．したがって特に任意の $u\in P$ に対し $V(u)\in K$ となる．一方 $u\in P$ に対しては，補題 14.4.3 より

$$V(u)\equiv u^n\prod_{i\in C_H(u)}d^*(u^{r_i})d^*(x_iu^{-r_i}x_i^{-1})$$

だった．ここで，定義より $d^*(u^{r_i})\in K$ であり，$v=x_iu^{-r_i}x_i^{-1}$ は H の p-元である．ゆえに適当な $y\in H$ をとると $y^{-1}vy\in P$ となり，補題 14.4.2 より $d^*(v)=v^{-1}d(v)=v^{-1}d(y^{-1}vy)$ となり，

$$d^*(v)\equiv v^{-1}y^{-1}vyd^*(y^{-1}vy)$$
$$\equiv(v,y)d^*(y^{-1}vy)$$

となる．ところが $(v,y)\in H'\subseteq H_0$ で，定義より $d^*(y^{-1}vy)\in K$ だから $d^*(v)=d^*(x_iu^{-r_i}x_i^{-1})\in K$ となる．ゆえに $u\in P$ に対し

$$u^n \equiv V(u) \in K$$

となるが，$(n, p)=1$ だからPの任意の元はPの適当な元のn乗になっている．よって $P \subseteq K$ となり，H/H_0 は p-群でPはHの Sylow p-部分群だから，$H=H_0 \cup P \subseteq K$，したがって $H=K$ がいえ，補題が証明された．

$G \lhd G_1$ で $H=H_1 \cap G$, $G \cup H_1 = G_1$ だから，G_1 における H_1 の左剰余類の代表系として，GにおけるHの左剰余類の代表系 $1, x_2, \cdots, x_n$ を使うことができる．すなわち $G_1=H_1+H_1x_2+\cdots+H_1x_n$ となる．したがって G_1 は H_1 と P_1 による両側剰余類を使って

$$G_1=H_1+H_1t_1P_1+\cdots+H_1t_sP_1$$

と書ける．ただし，$1, t_1, \cdots, t_s$ というのは $1, x_2, \cdots, x_n$ の部分集合である．$H_1t_iP_1$ における H_1 による剰余類上の P_1 の可移置換表現を $\pi_i(i=1, \cdots, s)$ とする．π_i の次数が1とすると $H_1t_iP_1=H_1t_i$ となり，$t_iP_1t_i^{-1} \subseteq H_1$ となるから，Sylow の定理により適当な $y \in H_1$ をとれば $t_iP_1t_i^{-1}=y^{-1}P_1y$ となり，$yt_i \in N_1 \subseteq H_1$，したがって $t_i \in H_1$ となるが，このようなことは起こらない．よって π_i の次数は1より大で，恒等表現ではない．したがってその核 K_i は P_1 に真に含まれ，π_i は P_1/K_i の忠実な表現となる．ところが P_1/K_i はp-群だからその中心は単位元だけではない．そこで $z_i \in P_1$ を $\pi_i(z_i)$ の位数がpで，$\pi_i(P_1)$ の中心に入るように選ぶことができる．すると任意の $u \in P_1$ に対し，$\pi_i(z_i)$ と $\pi_i(u)$ とは可換になる．可移置換群の中心の元が一点を固定すれば，すべての点を固定するから，$\pi_i(z_i)$ は $H_1t_iP_1$ のどの剰余類も固定せず，長さpの巡環だけからなる．任意の $u \in P \subseteq P_1$ に対し，$\pi_i(u)$ は $\pi_i(z_i)$ と可換だから，$\pi_i(u)$ が $H_1t_iP_1$ に含まれるある剰余類，たとえば H_1x_{j+1} を固定したとすると，H_1x_{j+1} の属する $\pi_i(z_i)$ の巡環のすべての剰余類 $H_1x_{j+1}, \cdots, H_1x_{j+p}$ を固定しなければならない．よって $u \in P$ に対し

$$d(u) \equiv u \cdot \prod d_j(u) \bmod H_0$$

と書くことができる．ただし

$$d_j(u)=h_1h_2\cdots h_p$$

で，

$$h_k = x_{j+k} u x_{j+k}^{-1}, \quad k=1, \cdots, p$$

である．ここで $x_{j+1}, \cdots, x_{j+p}$ は上と同じく，ある i に対する $\pi_i(z_i)$ の1つの巡環に現われる剰余類の代表元である．そして $u=1\cdot u\cdot 1^{-1}$ は $d(u)$ のうち H_1 から出てくる成分である．また $x_{j+k}ux_{j+k}^{-1}=h_k\in H_1$ であるが，$x_{j+k}\in G$, $u\in P$ より $h_k\in G$ となり，$h_k\in H_1\cap G=H$ となるから，これらは実際 $d(u)$ の成分として現われるものであることを注意しておく．そして $d^*(u)\equiv u^{-1}d(u)$ だから

$$d^*(u) \equiv \prod_j d_j(u) \bmod H_0$$

となり，この関係と補題 14.4.4 を使えば，直ちに次の補題が得られる．

補題 14.4.5. H は H_0 とすべての $u\in P$ に対する $d_j(u)$ の全体とで生成される．

これらの $d_j(u)$ のうちの1つをもっと詳しく調べることにしよう．簡単のため，$w_k=x_{j+k}, k=1, \cdots, p$ と書くことにする．添数を p を法として考えると

$$H_1 w_k z_i = H_1 w_{k+1}$$

が成り立つ．したがって適当な $y_k\in H_1$ により

$$w_k z_i = y_k w_{k+1}$$

となる．一方

$$w_k u w_k^{-1} = h_k, \quad d_j(u) = h_1 \cdots h_p$$

だった．よって

$$\begin{aligned} w_k(u, z_i)w_k^{-1} &= w_k u^{-1} w_k^{-1} \cdot w_k z_i^{-1} u z_i \cdot w_k^{-1} \\ &= h_k^{-1} y_{k-1}^{-1} w_{k-1} u w_{k-1}^{-1} \cdot w_{k-1} z_i w_k^{-1} \\ &= h_k^{-1} y_{k-1}^{-1} h_{k-1} \cdot y_{k-1} \\ &= h_k^{-1} h_{k-1} (h_{k-1}, y_{k-1}) \end{aligned}$$

となる．ところが $y_{k-1}\in H_1, h_{k-1}\in H$ で $(H_1, H)\subseteq H_0$ だから

$$w_k(u, z_i)w_k^{-1} \equiv h_k^{-1} h_{k-1} \bmod H_0$$

が成り立つ．さて，P は P_1 の正規部分群だから $(u, z_i)\in P$ で，$u_1=(u, z_i)$ に対して剰余類 $Hw_k, k=1, \cdots, p$ からの $d(u_1)$ の対角成分は $h_k^{-1}h_{k-1} \bmod H_0$,

$k=1, \cdots, p$ となる．以上より $w_k u w_k^{-1} \equiv h_k (\mathrm{mod}\ H_1), k=1, \cdots, p$ ならば，$w_k(u, z_i)w_k^{-1} \equiv h_k^{-1}h_{k-1} (\mathrm{mod}\ H_0), k=1, \cdots, p$ となることが分かった．そこで $u=u_0, u_1=(u, z_i), u_2=(u_1, z_i)$, 一般に $u_{s+1}=(u_s, z_i)$ と置く．もし

$$w_k u_s w_k^{-1} \equiv h_{k,s} (\mathrm{mod}\ H_0),\quad k=1, \cdots, p$$

ならば，

$$w_k u_{s+1} w_k^{-1} \equiv h_{k-1,s} h_{k,s}^{-1} \equiv h_{k,s+1} (\mathrm{mod}\ H_0)$$

となることが分かるから，s に関する帰納法により

$$w_k u_s w_k^{-1} \equiv h_{k-s} h_{k-s+1}{}^{-s} h_{k-s+2}{}^{\binom{s}{2}} \cdots h_k{}^{(-1)^s}$$

となることがわかる．ここで指数は１つおきに符号をかえた２項係数である．２項係数の性質と $H^p \subseteq H_0$ より

$$w_k u_{p-1} w_k^{-1} \equiv h_1 h_2 \cdots h_p \equiv d_j(u) \bmod H_0$$

となることが分かり[1)]，$u \in P$, $z_i \in P_1$ に対し

$$d_j(u) \equiv w_k(u, \overbrace{z_i, \cdots, z_i}^{p-1})w_k^{-1} (\mathrm{mod}\ H_0)$$

となる．そこで

$$e_p(u, z_i) = (u, \overbrace{z_i, \cdots, z_i}^{p-1})$$

と書くことにすると，すべての $u \in p$ について $x_{j+k} e_p(u, z_i) x_{j+k}^{-1}$ という形をした元で H に入るもの，すなわちすべての $u \in P$ と $i=1, \cdots, s$ について $e_p(x, z_i)$ の対角係数いくつかを H_0 につけ加えることにより H が得られることが補題 14.4.5 から分かる．これらの係数は H の p-元で，P は H の１つの Sylow p-部分群だから，これらの元を H の元で変換して P の元にすることができる．H/H_0 は可換群だからこの操作は H_0 を法として考えれば影響はない．

以上で主定理が証明された．

定理 14.4.1. (**P. Hall**). G_1 を任意の有限群，P_1 を１つの Sylow p-部分群，N_1 をその正規化群，H_1 を N_1 を含む部分群とする．$G=u_p(G_1)$ を位

1) $(-1)^m\binom{p-1}{m} = (-1)^m\binom{p}{m} + (-1)^{m-1}\binom{p-1}{m-1} \equiv 1 (\mathrm{mod}\ p)$ より

数が p と素な G_1 の元全体で生成される部分群とし，$H=G\cap H_1$, $N=G\cap N_1$, $P=G\cap P_1$ とおく．すると $u_p(H_1)=u_p(H)$ が成り立ち，もし $u_p(H)\neq H$ ならば，$H_0=H^p(H_1, H)u_p(H)$ は H の真部分群で，$e_p(u, z_i)=(u, \overbrace{z_i, \cdots, z_i}^{p-1})$ の共役で H に入るものいくつかを H_0 につけ加えることにより H が得られる．ただし $u\in P$ で，$z_i, i=1, \cdots, s$ は P_1 の元である．

$$G_1=H_1+H_1t_1P_1+\cdots+H_1t_sP_1$$

を G_1 の H_1 と P_1 による両側剰余類分解とし，$\pi_i, i=1, \cdots, s$ を $H_1t_iP_1$ における H_1 の剰余類上の P_1 の可移表現とすると，π_i の次数は1ではなく，z_i は $\pi_i(z_i)$ が位数 p で，$\pi_i(P_1)$ の中心に入るように選ぶ．

系 14.4.2. すべての $u, z\in P_1$ に対し $e_p(u, z)=1$ が成り立つならば，$u_p(N_1)=N=u_p(G_1)\cap N_1$ で $G_1/u_p(G_1)=N_1/u_p(N_1)$ となる．特に P_1 の級が p より小さい場合にはこのようなことが起こる．

$H_1=N_1$ と置けば $H=N$ となり，系が証明される．

Q_1 が P_1 の弱い意味で閉じている部分群だとしよう．するとすでに注意したように，Q_1 は P_1 の正規化群 N_1 の正規部分群となる．したがって N_1 を含む部分群 H_1 として Q_1 の正規化群をとることができる．すると前の定理は Wielandt [3] の定理の改良された結果を与える．

定理 14.4.2. (**Hall-Wielandt**). P_1 を G_1 の Sylow p-部分群，Q_1 を P_1 の弱い意味で閉じた部分群とし，P_1 の正規化群を N_1, Q_1 の正規化群を H_1 と置く．すると次の3つの条件のうちどれかが成り立てば，$u_p(H_1)=H=u_p(G_1)\cap H_1$ となり，したがって $G_1/u_p(G_1)=H_1/u_p(H_1)$ が成り立つ．

1) すべての $u\in P_1, z\in Q_1$ に対し $e_p(u, z)=1$ となる．

2) すべての $u, z\in Q_1$ に対し $e_{p-1}(u, z)=1$ となる．

3) P_1 の昇中心鎖の $(p-1)$ 番目の項 $Z_{p-1}(P_1)$ に Q_1 が含まれる．

証：定理 14.4.1 の証明のときと同様に，$H_1t_iP_1$ の剰余類上の P_1 の表現 π_i の核を K_i とする．もし $Q_1\subseteq K_i$ とすると $H_1t_iQ_1=H_1t_i$ となり，$t_iQ_1t_i^{-1}\subseteq H_1$

となる．したがって，$t_iQ_1t_i^{-1}$ は H_1 に含まれる p-部分群で，P_1 は H_1 の1つの Sylow p-部分群としたから，適当な $y\in H_1$ により $y^{-1}t_iQ_1t_i^{-1}y\subseteq P_1$ とできる．Q_1 は P_1 において弱い意味で閉じているとしたから $y^{-1}t_iQ_1t_i^{-1}y=Q_1$ となり，$y^{-1}t_i$ は Q_1 の正規化群 H_1 に含まれ，$t_i\in H_1$ となるが，このようなことは起こらない．ゆえに $Q_1\not\subseteq K_i$ である．Q_1 は P_1 の正規部分群だから，Q_1 の P_1/K_i における像は正規部分群となり，単位元と異なる中心の元を含まなければならない．したがって，z_i として Q_1 の元が選べる．このことから最初の条件が成り立てばよいことがわかる．u としては $P=P_1\cap G$ の元をとれば十分であるが，P_1 のどの部分群が P であるか前もってはわからないことを注意しておく．3番目の条件から最初の条件が出てくる．なぜなら，もし $Q_1\subseteq Z_{p-1}(P_1)$ とすると，$z\in Z_{p-1}(P_1)$ となり，したがって，$(u, z)\in Z_{p-2}(P_1)$, $(u, z, z)\in Z_{p-3}$ となる．これを続けていけば

$$e_p(u, z)=(u, \overbrace{z, \cdots, z}^{p-1})=1$$

となる．2番目の条件については，$u\in P_1$, $z\in Q_1$ に対して $u_1=(u, z)$ と置くと，$e_p(u, z)=e_{p-1}(u_1, z)$ となるから，やはり，2番目の条件から最初の条件が導かれる．

系 14.4.3. Q_1 を P_1 の特性部分群とする．もし Q_1 が P_1 において弱い意味で閉じていなかったとすると，Q_1 を含む別の Sylow p-部分群 P_2 で Q_1 が正規部分群でないようなものが存在する．Q_1 が定理の条件（1），（2）または（3）を満たし，$G_1/u_p(G_1)$ と $H_1/u_p(H_1)$ とが同型でないときにはこのようなことが起こる．

証：Q_1 は P_1 の特性部分群だから，N_1 の正規部分群となる．したがって，Q_1 の正規化群 H_1 は N_1 を含む．もし Q_1 が P_1 において弱い意味で閉じていなかったとすると，$x^{-1}Q_1x\subseteq P$ だが，$x^{-1}Q_1x\neq Q_1$ となる x が存在する．もし $x^{-1}Q_1x$ が P_1 の正規部分群だったとすると，補題 14.3.1 により Q_1 と $x^{-1}Q_1x$ は N_1 において共役になるが，そのようなことは起こらない．よって $x^{-1}Q_1x$ は

P_1 に含まれるが正規部分群ではない．したがって，Q_1 は $P_2=xP_1x^{-1}$ に含まれるが正規部分群ではない．特に Q_1 が定理の条件（1），（2）または（3）を満たしていて，定理の結論が成り立たないとすれば，Q_1 は P_1 において弱い意味で閉じていない．

以下の定理はいままでのものよりかなり基本的である．

定理 14.4.3. P を G の Sylow p-部分群，G' を G の交換子群とすると，$V_{G\to P}(G)\cong P/P\cap G'$ が成り立つ．

証：$V_{G\to P}(G)$ は G から P/P' への準同型で，P/P' は p-群だから，位数が p と素な元は，単位元に写される．ところが G は P と p 以外の素数についての Sylow 部分群とで生成されているから，$V(G)=V(P)$ となる．

$$G=P+Px_2+\cdots+Px_n$$

とすると，補題 14.4.1 により，$u\in P$ に対し

$$\begin{aligned} V(u) &\equiv \prod_{i\in C_P(u)} x_i u^{r_i} x_i^{-1} \bmod P' \\ &\equiv \prod_{i\in C_P(u)} u^{r_i}(u^{r_i}, x_i^{-1}) \bmod P' \\ V(u) &\equiv \prod_{i\in C_P(u)} u^{r_i} \\ &\equiv u^n \bmod G' \end{aligned}$$

となる．$(n, p)=1$ だから $u\in P, u\notin G'$ ならば $V(u)\not\equiv 1 \bmod G'$ となる．一方 $V(G)$ は可換群だから $V(G')\equiv 1$ である．よって $P\to V_{G\to P}(P)$ の核はちょうど $P\cap G'$ で，$V_{G\to P}(G)\cong P/P\cap G'$ が成り立つ．

定理 14.4.4.（**Grün [1] の第 1 定理**）．P を G の Sylow p-部分群とする．このとき

$$P^*=[P\cap N_G(P)']\bigcup_{z\in G}(P\cap z^{-1}P'z)$$

と置くと，$V_{G\to P}(G)\cong P/P^*$ が成り立つ．

証：定理 14.4.3 により $V_{G\to P}(G)\cong P/P\cap G'$ となることは分かっている．P^* の定義により P^* は $P\cap G'$ に含まれる部分群の結びであるから，$P^*\subseteq P$

$\cap G'$ が成り立つ．したがって，$P\cap G'\subseteq P^*$ を示さなければならない．$P\cap G'$ の元 u は P^* に入るということを，u の位数に関する帰納法で証明することにする．まず，明らかに $1\in P^*$ である．P による G の両側剰余類分解を

$$G=P+Py_2P+\cdots+Py_sP$$

とする．$u\in P\cap G'$ とすると，補題 14.4.1 により

$$V(u)\equiv\prod_{i\in C_P(u)}x_iu^{r_i}x_i^{-1}\bmod P'$$

となるが，このうち両側剰余類 PyP から出てくる成分は

$$w=\prod_k yv_ku^{r_k}v_k^{-1}y^{-1}$$

という形になる．ただし，$v_1=1$, $v_k\in P$ で，PyP における P の左剰余類の数を p^t とすると，$\sum_{\kappa}r_k=p^t$ である．$V(u)$ の成分 w を次の 2 つの場合に分けて考察することにする：Case 1，$t\geq 1$；Case 2，$t=0$ したがって $p^t=1$.

Case 1. この場合

$$w\equiv yu^{p^t}y^{-1}(\bmod yP'y^{-1})$$

であるが，$v_1=1$ に対応する成分 $yu^{p^b}y^{-1}$ は P に入り，$b\leq t$ だから $yu^{p^t}y^{-1}$ も P に入る．一方 w も P に入るから

$$w\equiv yu^{p^t}y^{-1}(\bmod P\cap yP'y^{-1})$$

となり，特に

$$w\equiv yu^{p^t}y^{-1}(\bmod P^*)$$

となる．ところが $u\in P\cap G'$ だから，$V(u)\equiv 1(\bmod P')$ で，$V(yu^{p^t}y^{-1})\equiv 1$ $(\bmod P')$ が成り立つ．$yu^{p^t}y^{-1}$ は P の元だから核 $P\cap G'$ に入る．$t\geq 1$ としたから $yu^{p^t}y^{-1}$ の位数は u の位数より小さく，帰納法の仮定により $yu^{p^t}y^{-1}$ $\in P^*$ となる．同じく帰納法により $u^{p^t}\in p^*$ となるから

$$w\equiv yu^{p^t}y^{-1}\equiv 1\equiv u^{p^t}(\bmod P^*)$$

が成り立つ．

Case 2. この場合 $PyP=Py$ となり，$Py\subseteq N_G(P)$ となる．

$$w\equiv yuy^{-1}\equiv u(\bmod N_G(P)')$$

より $w \equiv u(\mathrm{mod}\ P\cap N_G(P)')$ となり，特に $w\equiv u(\mathrm{mod}\ F^*)$ が成り立つ．よっていずれの場合においても Py_iP に含まれる P による左剰余類の数を p^{t_j} とし，それから出てくる成分を w_j とすると，

$$w_j \equiv u^{p^{t_j}}(\mathrm{mod}\ F^*)$$

が成り立ち，

$$V(u)\equiv u^n(\mathrm{mod}\ P^*)$$

となる．ここで $n=[G:P]$ は p と素である．$u\in P\cap G'$ ならば $V(u)\equiv 1$ であるから，$V(u)\in P'\subseteq P^*$ となり，$u^n\equiv 1(\mathrm{mod}\ F^*)$，したがって，$u\in P^*$ となり，これが証明すべきことであった．

定理 14.4.5.（**Grün の第2定理**）．G が p-正規ならば，G の商群で可換 p-群となるもののうち，最大のものは，Sylow p-部分群の中心の正規化群のそれに同型である．

証：P を G の1つの Sylow p-部分群，Z をその中心とする．$G'(p)$ を $G/G'(p)$ が可換 p-群となるような G の最小の正規部分群とする．$G'(p)$ の位数は G の位数のうち p の巾以外のすべての成分を含んでいなければならないから $G=G'(p)\cup P$ となる．$G^*=P\cup G'$ と置くと，$G'(p)\cup G^*=G$ だが，G^*/G' は p-元しか含まず，$G'(p)/G'$ は位数が p と素な元しか含まないので，$G^*\cap G'(p)=G'$ も成り立つ．したがって，定理 2.4.1 により $G/G'(p)$ $=G^*/G'=P/P\cap G'$ となる．N を P の正規化群，H を Z の正規化群とすると，Z は P の特性部分群だから，$H\supseteq N$ が成り立つ．そこで，$H'(p)$ を $H/H'(p)$ が可換 p-群となるような H の最小の正規部分群とすると，G と同様に $H/H'(p)=P/P\cap H'$ が成り立つ．したがって定理を証明するためには $P\cap G'=P\cap H'$ を示すことが必要である．$G\supseteq H$ より明らかに $G'\supseteq H'$，したがって，$P\cap G'\supseteq P\cap H'$ が成り立つから，$P\cap H'\supseteq P\cap G'$ を示せばよい．Grün の第一定理より

$$P\cap G'=(P\cap N')\bigcup_{x\in G}(P\cap x^{-1}P'x)$$

が成り立つが，$H\supseteq N$ より $P\cap H'\supseteq P\cap N'$ が成り立つ．よって任意の $x\in G$

に対し

$$P\cap H'\supseteq P\cap x^{-1}P'x$$

を示すことが必要である．$M=P\cap x^{-1}P'x$ と置くと，$Z\subseteq N_G(M)$ だが，$x^{-1}Zx$ は $x^{-1}Px$ の中心だから $x^{-1}Zx$ も $N_G(M)$ に含まれる．Z を含む $N_G(M)$ の Sylow 部分群を $R, x^{-1}Zx$ を含む $N_G(M)$ の Sylow 部分群を S とすると，適当な $y\in N_G(M)$ により，Z と $y^{-1}x^{-1}Zxy$ は R を含む G の同一の Sylow 部分群 Q に含まれる．p-正規性から Z と $y^{-1}x^{-1}Zxy$ は共に Q の中心となり一致する．よって $xy=h\in N_G(Z)=H$ となるが，$y\in N_G(M)$ だったから

$$\begin{aligned}M&=y^{-1}My=y^{-1}Py\cap y^{-1}x^{-1}P'xy\\&=y^{-1}Py\cap h^{-1}P'h\subseteq H'\end{aligned}$$

となる．よって $M=P\cap x^{-1}P'x\subseteq P\cap H'$ となり，定理が証明できた．

P. Hall の定理を使うと，Grün の第2定理から“可換”という条件を落とすことができる．

定理 14.4.6. **(Hall-Grün)** G が p-正規ならば，p-群となる G の商群の中で最大のものは，Sylow p-部分群の中心の正規化群のそれと同型になる．

証：定理 14.4.2 において，G_1 を G, P_1 を1つの Sylow p-部分群，Q_1 を P_1 の中心，H_1 を Q_1 の正規化群とする．G_1 が p-正規ということは Q_1 が P_1 において弱い意味で閉じているということだった．そして $Q_1=Z(P_1)$ だから，3番目の条件が成り立ち，$G_1/u_p(G_1)\cong H_1/u_p(H_1)$ となることが分かる．これらは極大商 p-群で定理が証明できた．

Burnside の定理も改良することができる．どういうとき，G の Sylow p-部分群 P が G のある商群と同型になるだろうか？ つまり，$G/u_p(G)=P$ となるのはいつか？ こうなったとし，$B=u_p(G)$ と置くと，B は位数が p と素な G の元の全体である．そして $B\cap P=1, B\cup P=BP=G$ が成り立っている．P の任意の部分群 Q に対し $B\cup Q=BQ$ は，Q および位数が P と素な元を全部含んでいる部分群である．そして，B は BQ の正規部分群である．$W=N_{BQ}(Q)$

と置くと，$W\cap B$ は位数が p と素な W の元の全体である．明らかに $W\cap B \lhd W$ かつ $Q\lhd W$ だから $W=(W\cap B)\times Q$ となる．ゆえに位数が p と素な元が Q を正規化すれば Q を中心化する．これは $G/u_p(G)\cong P$ となるための必要条件だが，十分条件でもあるということを証明しよう．この点で定理 14.3.1 の一般化になっている．

定理 14.4.7. 群 G の商群 $G/u_p(G)$ が Sylow p-部分群 P と同型になるためには，P の任意の部分群 Q に対し，位数が p と素な元が Q の正規化群にはいれば，Q の中心化群にはいることが必要十分である．

証：$G=P$ のときは明らかに成り立つから，G の位数に関する帰納法を使うことにする．まず G が p-正規となることを証明する．Z を P の中心とする．G が p-正規でないとすると，定理 14.4.2 の系により，Z を含む別の Sylow p-部分群 P_2 で Z が正規部分群とならないものが存在する．すると定理 4.2.5 により，位数が p と素なある元により正規化されるが中心化されないような P の部分群 Q が存在する．仮定よりこのようなことは起こらないから，G は p-正規でなければならない．H を Z の正規化群とすると定理 14.4.6 により，$G/u_p(G)\cong H/u_p(H)$ となる．H が G の真部分群だったとすると，帰納法により $H/u_p(H)\cong P$ となり定理は証明された．

したがって，$G=H$ と仮定してよい．したがって Z は G の正規部分群である．しかし位数が p と素な元によって正規化されるが中心化されないような p-群 Q/Z を G/Z が含んだとすると，逆像 Q についても同じことが成り立つから，G/Z についても帰納法の仮定が成り立ち，G/Z は正規部分群 K/Z でその商群が P/Z に同型になるようなものを含む．Z は K の正規部分群で，K/Z は位数が p と素だから Z は K の中心に入り，$K=Z\times K_1$ と書ける．ここで K_1 は位数が p と素である．そして $K_1=u_p(K)=u_p(G)$ は位数が p と素な元だけから成っており，$G/u_p(G)=P$ となるが，これが証明すべきことだった．

第15章　群の拡大とコホモロジー

15.1. 正規部分群と商群の合成

一般に，与えられた群Uを部分群として含む群GはUの**拡大**（extension）とよばれる．一般の群拡大は Reinhold Baer [11] によって研究された．しかし，ここではUがGの正規部分群となっている場合だけを考えることにする．

与えられた群Nを正規部分群として含み，商群 G/N が与えられた群Hと同型になる群Gを全部構成するという問題を最初に考えたのは Otto Schreier [1, 2] である．NとHの直積はこの性質を持っているので，このような群はいつでも少なくとも1つは存在する．

まず，このような群Gが与えられたとして，それを詳細に調べることにしよう．商群 $H\cong G/N$ の元を $1, u, v, \cdots, w$ で表わすことにする．Hの各元xはGにおけるNの1つの剰余類と対応している．そこで剰余類 $\bar{x}N$ がxと対応するように代表$\bar{x}$をGから選ぶことにする．ただしNの代表としてはGの単位元1を選んでおく．すると

(15.1.1)
$$G=N+\bar{u}N+\bar{v}N+\cdots+\bar{w}N$$

となり，準同型 $G\to H$ により

(15.1.2)
$$\bar{u}\to u,\ \bar{u}\in G, u\in H$$

となる．Nは正規部分群だから，

(15.1.3)
$$a\leftrightarrows \bar{u}^{-1}a\bar{u}=a^u,\ a\in N$$

という写像はNの自己同型である．GからHの上への準同型により，$\bar{u}\to u$, $\bar{v}\to v$ となるから，

(15.1.4)
$$\bar{u}\cdot\bar{v}=\overline{uv}(u, v)$$

となる $(u, v)\in N$ が存在する．(15.1.4) により定義された (u, v) の全体の

つくる集合を**因子団**（factor set）とよぶ．以上より G の構造の中には次の 4 つの構造がはいっているわけである．

1） 正規部分群 N.

2） 商群 H.

3） N の自己同型：$a \leftrightarrows a^u$, $a \in N$, $u \in H$.

4） 因子団 $(u, v) \in N$；$u, v \in H$.

(15.1.3) と (15.1.4) により定義された自己同型と因子団は，一般には，u に対応する剰余類 $\bar{u}N$ の代表元 $\bar{u}$ の選び方に依存することを強調しておく必要がある．

自己同型と因子団の満たさなければならない条件がいくつかある．(15.1.4) の両辺の元で $a \in N$ を変換すると，

(15.1.5) $$(a^u)^v = (u, v)^{-1}(a^{uv})(u, v)$$

が成り立つ．

また，G において $(\bar{u}\bar{v})\bar{w} = \bar{u}(\bar{v}\bar{w})$ が成り立っていて，

$$\begin{aligned}(\bar{u}\bar{v})\bar{w} &= [\overline{uv}(u, v)]\bar{w} \\ &= \overline{uv}\bar{w}(u, v)^w \\ &= \overline{uvw}(uv, w)(u, v)^w, \\ \bar{u}(\bar{v}\bar{w}) &= \bar{u}[\overline{vw}(v, w)] \\ &= \overline{uvw}(u, vw)(v, w)\end{aligned}$$

だから，

(15.1.6) $$(uv, w)(u, v)^w = (u, vw)(v, w)$$

が成り立つ．

G の 2 元 $\bar{u}a, \bar{v}b$ の積については，

$$(\bar{u}a)(\bar{v}b) = \bar{u}\bar{v}a^v b = \overline{uv}(u, v)a^v b$$

となり，

(15.1.7) $$(\bar{u}a)(\bar{v}b) = \overline{uv}(u, v)a^v b$$

が成り立つ．N の G における代表としては 1 をとるという約束だったから，(15.1.4) よりすべての $u, v \in H$ に対し

(15.1.8)
$$(u, 1)=1=(1, v)$$
が成り立つ．

逆に，自己同型と因子団が条件（15.1.5）と（15.1.6）を満たせば，Nを正規部分群としてもち，$G/N\cong H$ となるGが存在する．記号 $\bar{u}a, u\in H, a\in N$ の全体Gに

(15.1.9)
$$\bar{u}a\cdot\bar{v}b=\overline{uv}(u, v)a^v b$$
という規則により積を定義する．

$$\begin{aligned}(\bar{u}a\cdot \bar{v}b)\cdot\bar{w}c &= \overline{uv}(u, v)a^v b\cdot\bar{w}c\\ &= \overline{uvw}(uv, w)(u, v)^w(a^v)^w b^w c\\ &= \overline{uvw}(uv, w)(u, v)^w(v, w)^{-1}a^{vw}(v, w)b^w c \quad [(15.1.5)\text{より}]\\ &= \overline{uvw}(u, vw)a^{vw}(v, w)b^w c \quad [(15.1.6)\text{より}]\\ &= \bar{u}a\cdot\overline{vw}(v, w)b^w c\\ &= \bar{u}a\cdot(\bar{v}b\cdot\bar{w}c)\end{aligned}$$

が成り立つから，この積は結合的である．逆の証明には（15.1.5）と（15.1.6）の他に（15.1.8）の特別の場合である．

(15.1.10)
$$(1, 1)=1$$
を仮定した方が便利である．（これを仮定しなくても証明はできる．）(15.1.5) において $u=v=1$ と置き，(15.1.10) を使えば $(a^1)^1=a^1$ を得るが，$a^1=c$ は N の任意の元に取れるから，すべての $c\in N$ に対し $c^1=c$ が成り立つ．(15.1.6) において $u=v=1$ と置くと，$1=(1, 1)^w=(1, w)$ となる．同様に $v=w=1$ と置けば $(u, 1)=1$ となることが分かる．$\bar{1}1\cdot\bar{w}c=\bar{w}(1, w)c=\bar{w}c$，および $\bar{u}a\cdot\bar{1}1=\bar{u}(u, 1)a=\bar{u}a$ が成り立つから $\bar{1}1$ は G の単位元である．$a\leftrightarrows a^w$ はNの自己同型であるから，$c\in N$ と $w\in H$ が与えられたとき，$d^w=(w^{-1}, w)^{-1}c^{-1}$ を満たす N の元 d が存在する．ゆえに G の任意の元 $\bar{w}c$ に対し，$\overline{w^{-1}}d\cdot\bar{w}c=\bar{1}(w^{-1}, w)d^w c=\bar{1}1$ となる．したがって G の任意の元が左逆元を持ち，Gが群になることが証明された．積の規則（15.1.9）により

(15.1.11)
$$\bar{u}a\to u$$
という写像はGからHの上への準同型で，その核は $\bar{1}a$ という元の全体から成

っている．ところが，

$$\bar{1}a\cdot\bar{1}b=\bar{1}(1,1)ab=\bar{1}ab$$

となるから，$\bar{1}a \leftrightarrows a$ という同型写像によりこの核と N とが同一視できる．$\bar{u}1\cdot 1a=\bar{u}(u,1)a=ua$ であるから，N による剰余類の代表系として $\bar{u}=\bar{u}1$ をとることができ，$\bar{u}a$ を u と a の積とみなすことができる．

以上得られた結果を定理の形にまとめておく．

定理 15. 1. 1. (**Schreier**). 群 G と正規部分群 N および商群 $H=G/N$ が与えられたとする．剰余類の代表系 $\bar{u}$ を $\bar{1}=1, \bar{u}N\to u\in H$ となるようにとると，

$$(a^u)^v=(u,v)^{-1}(a^{uv})(u,v),\quad a,(u,v)\in N\ ;\ u,v\in H\ ;$$

$$(uv,w)(u,v)^w=(u,vw)(v,w)\ ;\ (1,1)=1$$

を満たすような自己同型と因子団が決まる．

逆に，すべての $u\in H$ に対し N の自己同型 $a\leftrightarrows a^u$ が与えられ，この自己同型と因子団 $[(u,v)\in N]$ $(u,v\in H)$ に対し上の条件が成り立つならば，$\bar{u}a, u\in H, a\in N$ という元の全体に

$$\bar{u}a\cdot\bar{v}b=\overline{uv}(u,v)a^v b$$

という規則により積を定義すれば，群 G が定義され，N はその正規部分群で $G/N\cong H$ が成り立つ．

$(1,1)=1$ という条件を落してもこの定理は $\bar{1}(1,1)^{-1}$ を G の単位元とすれば成り立つ．

$N, H, a\leftrightarrows a^u$ および因子団 (u,v) によって一意的に定まる拡大 G は $E[N, H, a^u, (u,v)]$ と表わされる．

N の G における剰余類の代表系をとりかえて

(15. 1. 12) $$\bar{\bar{u}}=\bar{u}\alpha(u),\quad u\in H,\quad \alpha(u)\in N$$

とする．ただし $\bar{\bar{1}}=\bar{1}=1$ にとるから $\alpha(1)=1$ である．このとき自己同型は

(15. 1. 13) $$a\leftrightarrows a^{u'}=\bar{\bar{u}}^{-1}a\bar{\bar{u}}=\alpha(u)^{-1}a^u\alpha(u)$$

に変わる．

因子団 (u, v) も

(15. 1. 14) $$\bar{\bar{u}}\cdot\bar{\bar{v}}=\bar{u}\alpha(u)\bar{v}\alpha(v)=\overline{uv}(u, v)\alpha(u)^v\alpha(v)$$
$$=\overline{\overline{uv}}(u, v)^1=\overline{uv}\alpha(uv)(u, v)^1$$

という規則により $(u, v)^1$ に置き換えられる.

定 義：2つの拡大 $E_1=E[N, H, a^u, (u, v)]$ と $E_2=[N, H, a^{u^1}, (u, v)^1]$ は自己同型と因子団が

$$a^{u^1}=\alpha(u)^{-1}a^u\alpha(u),$$
$$(u, v)^1=\alpha(uv)^{-1}(u, v)\alpha(u)^v\alpha(v)$$

という関係にあるとき同値であるという. ただし $\alpha(u)$ というのは N に値をとる $u\in H$ の関数で, $\alpha(1)=1$ を満たす. このとき

$$E[N, H, a^u, (u, v)]\sim E[N, H, a^{u^1}, (u, v)^1]$$

と書く.

E_2 が E_1 に同値であるということは, 同一の群 G において N の剰余類の代表系をとりかえることに等しいから, この関係は対称律, 反射律, 推移律を満たし, 本当に同値関係となっている.

N の G における剰余類の代表系 $\bar{\bar{u}}$ が

(15. 1. 15) $$\overline{\overline{uv}}=\bar{\bar{u}}\bar{\bar{v}}$$

を満たすように選べるとき, すなわち $(u, v)^1=1$ となるときは剰余類の代表系が H と同型な群を作り, H と同一視できる. このとき G は N 上分解する, G は N と H の半値積であるなどという.

定理 15. 1. 2. 拡大 $G=E[N, H, a^u, (u, v)]$ が N 上分解するためには, すべての $u, v\in H$ に対し

$$(u, v)\alpha(u)^v\alpha(v)=\alpha(uv)$$

を満たすような関数 $\alpha(u)\in N, u\in H$ が見つかることが必要十分である.

証：$\bar{\bar{u}}$ を $G=E[N, H, a^u, (u, v)]$ が N 上分解するような剰余類の代表系とすると, $(u, v)^1=1$ となり, $\bar{\bar{u}}=\bar{u}\alpha(u)$ とすると,

(15. 1. 16) $$(u, v)\alpha(u)^v\alpha(v)=\alpha(uv)$$

という関係が成り立つことが分かる.

逆に, (15.1.6) が成り立つような関数 $\alpha(u)$ が存在したとし, a^{u^1} を $a^{u^1} = \alpha(u)^{-1}a^u\alpha(u)$, $\bar{\bar{u}} = \bar{u}\alpha(u)$ で定義すると, $E[N, H, a^u, (u, v)]$ と同値な拡大 $E[N, H, a^{u^1}, (u, v)^1] = G$ が存在し, すべての $u, v \in H$ に対し $(u, v)^1 = 1$ を満たす. ゆえに拡大GはN上分解する.

15.2. 中 心 拡 大

群Aの群Hによる拡大において, すべての因子 (u, v) がAの中心Bにはいっていると仮定しよう. このとき $E[A, H, a^u, (u, v)]$ はAのHによる**中心拡大** (central extension) とよばれる. 特にAが可換群ならば $B=A$ だから, A のすべての拡大は中心拡大である.

中心拡大に対しては, (15.1.5) は

(15.2.1) $$(a^u)^v = a^{uv}$$

となり, これは自己同型 $a \leftrightarrows a^u$ の全体がHに準同型な群をつくるということを意味している. χ というのをHの各元にAの自己同型を対応させる1つの特別な方法で, このような自己同型の全体がHに準同型な群をつくるとする. さらに剰余類の代表系 $\bar{u}$ をBにはいる因子 $\alpha(u)$ で変えても自己同型は不変であるとする. Baer [1] により $H-\chi$ 拡大とよばれるこのような拡大では自己同型は固定されていて, それらの全体はHに準同型な群をつくっている. これで中心拡大に対する条件 (15.1.5) は片付いたわけで,

(15.2.2) $$(uv, w)(u, v)^w = (u, vw)(v, w)$$

だけを考えればよいわけである. ただし同値な拡大というのは,

(15.2.3) $$(u, v)^1 = \alpha(uv)^{-1}(u, v)\alpha(u)^v\alpha(v)$$

が成り立つような $\alpha(u) \in B$ が存在することである.

因子団 $(u, v)_1$ と $(u, v)_2$ が共に (15.2.2) を満たしたとすると,

(15.2.4) $$(u, v)_3 = (u, v)_1(u, v)_2, \quad u, v \in H$$

と定義すれば, $(u, v)_3$ も (15.2.2) を満たし, Aの $H-\chi$ 拡大を定める1つの因子団となる. 因子団の積をこのように定義すると, すべての $(u, v)=1$ と

いう因子団が単位元で，(u, v) を $(u, v)^{-1}$ で置き換えたものが逆元となる．さらに同値な因子団に対しては，$(u, v)_1{}^* \sim (u, v)_1$, $(u, v)_2{}^* \sim (u, v)_2$ とすれば $(u, v)_1{}^*(u, v)_2{}^* \sim (u, v)_1(u, v)_2$ となる．ゆえにすべての $H-\chi$ 因子団は同値な因子団を同一視すれば，1つの可換群をつくり，**拡大の群** (group of extensions) とよばれる．

Hが有限群のとき，

(15. 2. 5)
$$f(v) = \prod_u (u, v)$$

と定義し，すべての $u \in H$ について (15. 2. 2) を掛けあわせると，H の位数を n とするとき

(15. 2. 6)
$$f(w)f(v)^w = f(vw)(v, w)^n$$

が得られる．(15. 2. 3) と比べてみると

(15. 2. 7)
$$(v, w)^n \sim 1$$

となることが分かる．また，mがBの任意の元の位数の倍数になっているとすると，$(u, v) \in B$ だから

(15. 2. 8)
$$(v, w)^m = 1$$

となる．ゆえに次の定理が成り立つ．

定理 15. 2. 1. 拡大の群の任意の元の位数はHの位数およびBの元の位数の最小公倍数を割り切る．

系 15. 2. 1. mとnが互いに素ならば，Aのすべての $H-\chi$ 拡大はAのHによる半直積に同値である．

この定理の応用として，中心拡大とは限らない一般の拡大に関する定理15. 2. 2 が証明できる．

定理15. 2. 2.[1] Gを位数mの正規部分群Kと位数nの商群 $H=G/K$ を持つ位数 mn の有限群とし，mとnが互いに素とする．このときGはK上分解する．

---

[1] Schur の定理または Schur-Zassenhaus の定理と呼ばれる．

証：Gが位数nの部分群を持つことを示せばよい．nに関する帰納法を行なう．$m=1$のときは明らかに定理は成り立つ．$m>1$とし，pをmを割り切る1つの素数とする．Gの Sylow p-部分群 S_p はすべてKの部分群である．なぜならKは少なくとも1つは Sylow 部分群S_pを含み，Kは正規部分群だから，S_pの共役もKにはいる．よって Sylow p-部分群の数はGにおいてもKにおいても同じである．ゆえに定理1.6.1により $[G:N_G(S_p)]=[K:N_K(S_p)]$，したがって $[N_G(S_p):N_K(S_p)]=[G:K]=n$ となる．ただし $N_G(S_p)$ および $N_K(S_p)$ はS_pのGおよびKにおける正規化群である．もちろん $N_K(S_p)=N_G(S_p)\cap K$であるから，定理2.4.1により $N_K(S_p)$ は $N_G(S_p)$ の正規部分群である．もし $N_G(S_p)$ がGの真部分群ならば，帰納法により位数nの部分群を含む．

ゆえに $G=N_G(S_p)$，したがって $K=N_K(S_p)$ と仮定してよい．もし S_p がKの真部分群ならば，帰納法によりGは G/S_p に同型な位数 $[G:S_p]$ の部分群を含み，したがって G/K に同型な位数nの部分群を含むことになり，定理が証明される．ゆえに我々の証明は $K=S_p$ という場合に帰着された．もし S_p が可換群ならばGは S_p の中心拡大で，定理15.2.1の系によりGは S_p 上分解し，定理が証明される．もし S_p が可換群でなければ S_p の中心Zは S_p の真部分群で，S_p の特性部分群であるから G の正規部分群になる．よって帰納法により G/Z は位数nの部分群 U/Z を含む．ところが Z はUの指数nの正規部分群であるから，帰納法によりUは位数nの部分群を含み，この最後の場合についても定理は証明された．

15.3. 巡 回 拡 大

Hを元xで生成された位数mの有限巡回群とする．Hの元は

(15.3.1)　$$1, x, x^2, \cdots, x^{m-1}$$

である．$G/N=H$ のとき，xに写されるNの剰余類の代表元を $\bar{x}$ とすると，$x^2, \cdots, x^{m-1}$ に写される剰余類の代表元として $\bar{x}^2, \cdots, \bar{x}^{m-1}$ がとれ，

(15.3.2)　$$G=N+N\bar{x}+\cdots+N\bar{x}^{m-1}$$

となる．そして

(15. 3. 3) $$\bar{x}^m=\alpha$$

はNの元である．

したがって N の自己同型 $a \leftrightarrows a^x$ については，その m 乗を考えると，

(15. 3. 4) $$a^{x^m}=\alpha^{-1}a\alpha,\quad \alpha\in N$$

が成り立つ．

さらに恒等式

(15. 3. 5) $$\bar{x}^{-1}\bar{x}^m\bar{x}=\bar{x}^m$$

より

(15. 3. 6) $$\alpha^x=\alpha$$

を得る．

NのHによる拡大を定義するためには（15. 3. 4）と（15. 3. 6）だけが必要であることを証明しよう．

定理 15. 3. 1. Hを位数mの有限巡回群とする．このときNのHによる拡大Gが存在するためには，Nの１つの自己同型 $a \leftrightarrows a^x$ と１つの元 $\alpha\in N$ で，次の条件（１），（２）を満たすものが存在することが必要十分である．

（１） この自己同型の m 乗は α による変換で与えられるNの内部自己同型である．

（２） この自己同型により α は固定される．

証：拡大が存在すれば自己同型 $a \leftrightarrows a^x$ と元αは (15. 3. 4) と (15. 3. 6) を満たすことはすでに示した．逆に１つの拡大を決めるのに (15. 3. 4) と (15. 3. 6) で十分であることを示さなければならない．H の元は $1, x, \cdots, x^{m-1}$ である．自己同型を

(15. 3. 7) $$a^{x^0}=a,\ a^{x^i}=(a^{x^{i-1}})^x,\ i=1, \cdots, m-1$$

と定義し，因子団を

(15. 3. 8. 1) $$i+j\leq m-1 \text{ なら } (x^i, x^j)=1,$$

(15. 3. 8. 2) $$m\leq i+j \text{ なら } (x^i, x^j)=\alpha$$

と置く．このように定義すれば，（15. 1. 5）と（15. 1. 6）が満たされることが

容易に分かり，定理 15.1.1 により 1 つの拡大が定義される．

H が無限巡回群のときには，すべての i, j に対し $(x^i, x^j)=1$ と置けばよく，自己同型 $a \leftrightarrows a^x$ には何も制限がつかないことが分かる．これはすべての i に対し $x^i=\bar{x}^i$ とおくということと同じである．

15.4. 定義関係式と拡大

前節では，Hが巡回群のときには，Hの定義関係式が特に簡単であることに対応して，群Nを拡大するための条件が特に簡単になることが分かった．この節では，もっとも一般の群Hについて，拡大の条件が定義関係式にどのように関係するかを見ることにしよう．

群Hが生成元 $x, y, z, \cdots$ と関係

(15.4.1) $$\phi_i(x, y, z, \cdots)=1 \qquad i=1, 2, \cdots, r$$

で与えられたとする．H の各元 h は生成元とその逆元についての決まった語 $h=h(x, y, z, \cdots)$ で表わされていると思ってよい．GをNのHによる拡大とすると，N による剰余類の代表元として $\bar{x}, \bar{y}, \bar{z}, \cdots$ についての対応する語をとり，準同型 $G \to H$ において

(15.4.2) $$\begin{gathered} G \to H \\ \bar{x} \to x \\ h(\bar{x}, \bar{y}, \cdots) \to h(x, y, \cdots) \end{gathered}$$

となるようにできる．$x, y, z, \cdots$ に対応する生成元 $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \cdots$ を持つ自由群を F_1 とする．すると，

(15.4.3) $$\begin{gathered} \boldsymbol{x} \to \bar{x} \to x, \\ \boldsymbol{y} \to \bar{y} \to y, \\ \cdots\cdots\cdots\cdots \end{gathered}$$

で定義される準同型により

(15.4.4) $$F_1 \to \bar{H} \to H$$

と写される．ここで $\bar{H}$ というのは $\bar{x}, \bar{y}, \bar{z}, \cdots$ で生成される G の部分群で，N の各剰余類の元を少なくとも 1 つずつ含んでいる．ゆえに $G=\bar{H} \cup N$ とな

る．したがって F_2 を N を準同型像として持つような自由群とすると，自由群 $F=F_1\cup F_2$ をとり，準同型

(15.4.5) $$F\to G\to H,\quad F=F_1\cup F_2$$
$$F_1\to \bar{H}\to H,$$
$$F_2\to N\to 1$$

を定義できる．$\bar{H}$ の各元 $\bar{h}$ は変換により，N の自己同型

(15.4.6) $$\bar{h}^{-1}a\bar{h}=a^h,\quad \bar{h}\in H,\quad a\in N$$

を引き起こす．写像 $F_1\to H$ において，$\phi_i(\boldsymbol{x}, \boldsymbol{y}, \cdots)$ を含む最小の正規部分群を W とすると $H=F_1/W$ が成り立つ．ゆえに $\bar{H}\to H$ において，$\phi_i(\bar{x}, \bar{y}, \cdots)\to 1$, したがって

(15.4.7) $$\phi_i(\bar{x}, \bar{y}, \cdots)=\alpha_i\in N$$

となる．

自由群 F において恒等式

$$u_1u_2\cdots u_r=z_1z_2\cdots z_s$$

が成り立つのは，両辺の既約形式が同じになるときである．F から G の上への写像において恒等式はそのまま保たれる．特に，W と F_2 は N の元の上に写される．したがって W と F_2 によって生成される正規部分群での恒等式があれば，(15.4.6) と (15.4.7) という規則によって，α_i や自己同型 $a\leftrightarrows a^h$ に関する条件に置き換えられ，それは N の H による拡大 G が存在するための条件と解釈される．$\overline{uv}^{-1}\bar{u}\bar{v}$ は $N\cap\bar{H}$ に入るから W の元の G における像で，$\phi_i(\bar{x}, \bar{y}, \cdots)=\alpha_i$ の共役の積として表わされる．ゆえに各因子 $(u, v)=\overline{uv}^{-1}\bar{u}\bar{v}$ は W の元の $\bar{H}$ における像で，$\bar{u}=h_1(\bar{x}, \bar{y}, \cdots)$, $\bar{v}=h_2(\bar{x}, \bar{y}, \cdots)$, $\overline{uv}=h_3(\bar{x}, \bar{y}, \cdots)$ ならば (u, v) は W の元

(15.4.8) $$h_3(\boldsymbol{x}, \boldsymbol{y}, \cdots)^{-1}h_1(\boldsymbol{x}, \boldsymbol{y}, \cdots)h_2(\boldsymbol{x}, \boldsymbol{y}, \cdots)$$

の像となる．

定理 15.1.1 の条件というのは (15.4.6) と (15.4.7) により，因子団と自己同型についての条件に置き換えられた F での恒等式である．したがって (15.1.5) の

$$(a^u)^v=(u,v)^{-1}(a^{uv})(u,v)$$

は，自己同型について (15.4.6) を使い，W の元を N の元で置き換えることにより，恒等式

(15.4.9) $$\bar{v}^{-1}(\bar{u}^{-1}a\bar{u})\bar{v}=(\overline{uv}^{-1}\bar{u}\bar{v})^{-1}(\overline{uv}^{-1}a\overline{uv})(\overline{uv}^{-1}\bar{u}\bar{v})$$

を言い換えたものである．同様に (15.1.6) の $(uv,w)(u,v)^w=(u,vw)(v,w)$ は恒等式

(15.4.10) $$(\overline{uvw}^{-1}\overline{uv}\bar{w})\bar{w}^{-1}(\overline{uv}^{-1}\bar{u}\bar{v})\bar{w}=(\overline{uvw}^{-1}\bar{u}\overline{vw})(\overline{vw}^{-1}\bar{v}\bar{w})$$

を言い換えたものである．したがってNのHによる拡大が存在するための条件はFでの恒等式を言い換えたものである．この条件の中にNの定義関係式がはいらないことを注意しておく．この条件はNの元 α_i とNの自己同型でHの定義関係式と両立するものを見つけることとみなせる．これらの条件はHが自由群のときには無意味となる．なぜなら，常に $\overline{uv}=\bar{u}\bar{v}$ と置き，単位元を因子団にとることができ，自己同型が群をつくることだけが必要だからである．

実際問題としては拡大の存在のための条件を導き出すようなFの恒等式を決定するのは難しい問題であるが，NのHによる中心拡大の場合に，そのような決定の1つを次節で行なうことにする．

15.5. 群環と中心拡大*)

中心Cを持つ群Nの有限群Hによる中心拡大を考えることにしよう．§15.2と同様に，自己同型は

(15.5.1) $$(a^u)^v=a^{uv}$$

を満たすとする．因子 $(u,v)=\overline{uv}^{-1}\bar{u}\bar{v}$ は C にはいると仮定した．補題7.2.2を（左剰余類でなく右剰余類について）適用すると，これらの元は $\bar{H}/T=H$ となる $\bar{H}$ の部分群 T を生成する．そして

(15.5.2) $$\phi_i(x,y,\cdots)=1$$

をHの定義関係式とすると，

(15.5.3) $$\phi_i(\bar{x},\bar{y},\cdots)=\alpha_i\in C$$

*) M. Hall, Jr. [1] 参照.

となる．なぜなら，α_i はTに属し，TはCの元で生成されているからである．

Cの自己準同型rとsに対し，

$$a^r a^s = a^{r+s} \tag{15.5.4}$$

という規則により，自己準同型 $r+s$ を定義することができる．したがって(15.5.1)と(15.5.4)より，Hの群環H^*はCの作用環となる．ただし群環H^*というのは

$$c_1 h_1 + \cdots + c_n h_n \tag{15.5.5}$$

という形の元全体で，$h_1, \cdots, h_n$ はHの元，$c_1, \cdots, c_n$ は整数である．H^*の元の和は係数を加えることで，H^*の元の積はHでの乗法 $h_i h_j = h_k$ と２つの分配法則から与えられる．H^*が結合的な環になり，Hの単位元がH^*の単位元となることは容易に確かめられる．

H^*を作用環としてもつ可換群Aは，Aのすべての元が

$$a = a_1^{z_1} a_2^{z_2} \cdots a_r^{z_r} \qquad z_i \in H^* \tag{15.5.6}$$

という形に一意的に書けるような基底 $a_1, a_2, \cdots, a_r$ を持つとき，**作用自由** (operator free) とよばれる．したがって$a=1$ ならば，$z_1 = z_2 = \cdots = z_r = 0$ となる．

定理 15.5.1. 作用自由な群Aの有限群Hによる拡大GはAのHによる半直積だけである．

証：Aのすべての元bは

$$b = a_1^{z_1} \cdots a_r^{z_r} \qquad z_i \in H^*$$

と一意的に表わされる．そこで $z_i = c_{i1} h_1 + \cdots + c_{in} h_n$, $i = 1, \cdots, r$ とし，

$$(b\,;\,h_j) = a_1^{c_{1j}} a_2^{c_{2j}} \cdots a_r^{c_{rj}}$$

と置くと，$t = h_1, h_2, \cdots, h_n$ を動かしたとき，bは

$$b = \prod_t (b\,;\,t)^t \qquad t = h_1, \cdots, h_n \tag{15.5.7}$$

と一意的に表わされる．したがって因子団については

$$(u, v) = \prod_t (u, v\,;\,t)^t \tag{15.5.8}$$

となり，(15.5.7) の一意性により，(15.1.6) は

(15.5.9) $$(uv, w\,;t)(u, v\,;tw^{-1})=(u, vw\,;t)(v, w\,;t)$$

となる．そこでHのすべての元uに対し $\bar{\bar{u}}=\bar{u}\prod_t (u, t^{-1}\,;1)^{-t}$ と置き，(15.5.9) を代入して計算すれば，

(15.5.10) $$\bar{\bar{u}}\bar{\bar{v}}=\overline{\overline{uv}}$$

となることが確かめられる．したがってこの新しい代表系は群をつくり，GはAとHの半直積となる．

§15.4の結果によると，群Nの群Hによる中心拡大の条件は (15.5.1) と

(15.5.11) $$\prod_t \alpha_i{}^{u_i}=1 \qquad u_i\in H^*$$

という形の条件である．ただし，(15.5.3) と同じく $\phi_i(\bar{x}, \bar{y}, \cdots)=\alpha_i$ と置く．Nが作用自由な群だとしよう．$\alpha_i=1, i=1, \cdots, r$ と置くと1つの解が得られ，他の解は代表系をとりかえることによって得られるということは分かっていた．$\bar{x}=\xi\bar{\bar{x}}, \bar{y}=\eta\bar{\bar{y}}, \cdots$ と置くと，$\phi_i(\xi\bar{\bar{x}}, \eta\bar{\bar{y}}, \cdots)=1$ となる．そこで

(15.5.12) $$\alpha\bar{\bar{z}}=\bar{\bar{z}}\alpha^z,\ \ \alpha\in N$$

という規則を使うと，

(15.5.13) $$1=\phi_i(\xi\bar{\bar{x}}, \eta\bar{\bar{y}}, \cdots)=\phi_i(\bar{\bar{x}}, \bar{\bar{y}}, \cdots)\xi^{x_i}\eta^{y_i}\cdots$$

と書くことができる．したがって $\alpha_i{}^{-1}=\xi^{x_i}\eta^{y_i}\cdots$ も半直積の代表系をとりかえることによって得られるのだから条件 (15.5.11) を満たさなければならない．$\xi, \eta, \cdots$ をNの独立な基底元にとると，H^*において成り立つ次の方程式を得る．

(15.5.14) $$\sum_i x_iu_i=0,\ \sum_i y_iu_i=0, \cdots, \quad i=1, \cdots, r.$$

H^*の元 $x_i, y_i, \cdots$ は (15.5.12) という規則を使って，Hの定義関係式 $\phi_i(x, y, \cdots)=1$ から容易に計算でき，(15.5.11) の u_i は H^* の元で (15.5.14) を満たすものに制限される．逆に (15.5.14) を満たす u_i から条件 (15.5.11) が導き出すことができれば，条件 (15.5.11) の決定を (15.5.14) を解くことに帰着できたことになる．ここで与える証明は W. Magnus [2] による方法である．

定理 15.5.2. 群HとNが与えられたとする．NのHによる中心拡大が存在するための条件は，Hの元に付随した自己同型 $a \leftrightarrows a^h$ が（15.5.1）を満たし，Hの定義関係式を $\phi_i(x, y, \cdots)=1$ とするとき，$\phi_i(\bar{\bar{x}}, \bar{\bar{y}}, \cdots)=\alpha_i, i=1, \cdots, r$ を満たすNの中心Cの元 α_i が存在し，u_i を（15.5.14）を満たすH^*の任意の元とするとき，この α_i について（15.5.11）が成り立つことである．

証：いままでの議論により，（15.5.14）を満たす u_i の集合が条件（15.5.11）を決定すること以外はすべて示された．

§15.4と同様に，$\boldsymbol{x}, \boldsymbol{y}, \cdots$ で生成される自由群 F_1 を考え，$\phi_i(\boldsymbol{x}, \boldsymbol{y}, \cdots)$ を含む最小の正規部分群をWとして $H=F_1/W$ と置く．W'をWの交換子群とする．するとW'はWの特性部分群であるから F_1 の正規部分群となる．そして $T=F_1/W'$ は次の性質をもつ群である：（1）Tは $\bar{x}, \bar{y}, \cdots$ で生成され；（2）$V=W/W'$ はTの正規部分群で $T/V=H$ となり；（3）Vは可換群である．逆に，このような性質をもつ任意の群は F_1 の準同型像で，しかも W' の元は単位元に写されなければならないから，明らかにTの準同型像となる．次の補題を定理の証明に使うことにし，補題の証明は定理の証明が終ってからにする．

補題 15.5.1. hをHの元，LをH^*の元を係数とするいくつかの不定元についての線形形式とするとき，$\begin{pmatrix} h, & 0 \\ L, & 1 \end{pmatrix}$ という形の行列の積を

$$\begin{pmatrix} h_1, & 0 \\ L_1, & 1 \end{pmatrix}\begin{pmatrix} h_2, & 0 \\ L_2, & 1 \end{pmatrix}=\begin{pmatrix} h_1h_2, & 0 \\ L_1h_1+L_2, & 1 \end{pmatrix}$$

という規則で与えることにする．すると，$x, y, \cdots$ に対応する行列 $\bar{x}=\begin{pmatrix} x, & 0 \\ t_x, & 1 \end{pmatrix}$, $\cdots$ で，$T=F_1/W'$ に同型な群を生成するものが存在する．

$\begin{pmatrix} 1, & 0 \\ L, & 1 \end{pmatrix}$ という形の行列は加法的な群，したがって可換群を生成するから，T の準同型像となることを注意しておく．

中心拡大において，$\bar{H}$ はTの像になる．したがってTにおいて

$$\prod_i \phi_i(\bar{x}, \bar{y}, \cdots)^{u_i}=1, \quad u_i \in H^* \tag{15.5.15}$$

という関係が成り立てば，対応する関係（15.5.11）が $\bar{H}$ において成り立たなければならない．

補題を仮定すると，T において V の元として

(15.5.16)
$$\phi_i(\bar{x}, \bar{y}, \cdots)=\begin{pmatrix}1, & 0\\ L_i, & 1\end{pmatrix} \qquad i=1, \cdots, r$$

が成り立つ．ただし L_i は H^* の元を係数とする $t_x, t_y, \cdots$ についての線形形式である．$t_\xi, t_\eta, \cdots$ を新しい不定元とし，V に

(15.5.17)
$$\xi=\begin{pmatrix}1, & 0\\ t_\xi, & 1\end{pmatrix},\quad \eta=\begin{pmatrix}1, & 0\\ t_\eta, & 1\end{pmatrix}, \cdots$$

をつけ加えよう．$\bar{u}$ は前と同じとすると（$u\in H$），

(15.5.18)
$$\bar{u}^{-1}\xi\bar{u}=\begin{pmatrix}1, & 0\\ t_\xi u, & 1\end{pmatrix}$$

が成り立つ．

ゆえに（15.5.17）の元を V につけ加えることにより，作用自由な群をつけ加えたことになる．そして

(15.5.19)
$$\xi\bar{x}=\begin{pmatrix}x, & 0\\ t_\xi x+t_x, & 1\end{pmatrix}$$

が成り立つ．ゆえに（15.5.16）の L_i において t_x を $t_\xi x+t_x$ に置き換えることにより，$\phi_i(\xi\bar{x}, \eta\bar{y}, \cdots)$ が得られる．ゆえに

(15.5.20)
$$\phi_i(\xi\bar{x}, \eta\bar{y}, \cdots)=\phi_i(\bar{x}, \bar{y}, \cdots)\xi^{x_i}\eta^{y_i}\cdots$$

と，L_i の線形性より

(15.5.21)
$$\xi^{x_i}\eta^{y_i}\cdots=\begin{pmatrix}1, & 0\\ L_i(t_\xi x), & 1\end{pmatrix}$$

となることが分かる．ゆえに（15.5.14）の方程式 $\sum_i x_iu_i=0, \cdots$ が成り立てば

(15.5.22)
$$\sum L_i(t_\xi x)u_i=0$$

が成り立つ．t_ξ はどんな関係も満たさない不定元だったから，L_i の変数が何であっても

(15.5.23)
$$\sum_i L_iu_i=0$$

とならなければならない．これを（15.5.16）に適用すると

$$\prod_i \phi_i(\bar{x}, \bar{y}, \cdots)^{u_i}=1 \tag{15.5.24}$$

となることが分かる．この関係はTにおいて成り立つから，$\bar{H}$においても成り立ち，これで（15.5.14）が成り立てば，$\bar{H}$において $\prod \alpha_i{}^{u_i}=1$ となることが示された．ゆえに（15.5.11）は（15.5.14）の帰結であって，補題が証明されれば定理の証明が終る．

補題の証：$H=F_1/W$ とし，W の剰余類の代表系は F_1 の元の辞書式順序に関し，できるだけ前のものが選ばれているとしよう．すると同じ辞書式順序が H にも持ち込まれ，$\boldsymbol{h}=h(\boldsymbol{x}, \boldsymbol{y}, \cdots)$ が剰余類 $W\boldsymbol{h}$ の中で最初の元とすると，$h=h(x, y, \cdots)\in H$ はhの最初の辞書式表現として標準的な形である．ゆえにHの元や対応するWの剰余類の代表元に対しても同様の形が使え，Hの元の長さということが標準的な形の長さとして意味を持つ．そこで，$x, y, \cdots$ をHの生成元とし，

$$\bar{x}\to\begin{pmatrix}x, & 0\\ t_x, & 1\end{pmatrix},\quad \bar{y}\to\begin{pmatrix}y, & 0\\ t_y, & 1\end{pmatrix}$$

という行列との対応を考えよう．ただし，$h_1, h_2\in H$, L_1, L_2 を H^* の元を係数とする $t_x, t_y, \cdots$ についての線形形式とするとき

$$\begin{pmatrix}h_1, & 0\\ L_1, & 1\end{pmatrix}\begin{pmatrix}h_2, & 0\\ L_2, & 1\end{pmatrix}=\begin{pmatrix}h_1h_2, & 0\\ L_1h_2+L_2, & 1\end{pmatrix}$$

という規則により積をつくるとする．前にも注意したように，これらの行列から生成される群をKとするとき，$\begin{pmatrix}h, & 0\\ L, & 1\end{pmatrix}\to h$ は，KからHの上への準同型で，この準同型の核は $\begin{pmatrix}1, & 0\\ L, & 1\end{pmatrix}$ という形の元から成り，それは加法的な可換群をつくっていたから，Kは少なくともTの準同型像である．

定理7.2.3によりWは F_1 の自由部分群で，$\boldsymbol{x}$ を F_1 の生成元とするとき

$$\boldsymbol{c}_{ij}=\boldsymbol{h}_i\boldsymbol{x}\boldsymbol{h}_j{}^{-1}\neq 1,\quad \boldsymbol{h}_j=\phi(\boldsymbol{h}_i\boldsymbol{x}) \tag{15.5.25}$$

と置くと，$\boldsymbol{c}_{ij}$ が F_1 における自由生成系になる．

さらに補題7.2.3により $\boldsymbol{h}_i$ は $\boldsymbol{x}^{-1}$ では終らないし，$\boldsymbol{h}_j$ は $\boldsymbol{x}$ では終らない．群 W' は $\boldsymbol{c}_{ij}$ の交換子全体により与えられる群で，W/W' はW'を法として $\boldsymbol{c}_{ij}$ を基底とする自由可換群である．したがって，もし $\bar{h}_i\bar{x}\bar{h}_j{}^{-1}$ に対応する元

c_{ij} がKにおいて独立であることが示せれば，Kが $T=F_1/W'$ の忠実な表現であることが分かる．写像 $F_1\to H$ において $\boldsymbol{c}_{ij}\to 1$, $\boldsymbol{h}_i\to h_i$, $\boldsymbol{h}_j\to h_j$, $\boldsymbol{x}\to x$ であるから，Hにおいて $h_ix=h_j$ が成り立つ．そこで

$$\bar{h}_i\to\begin{pmatrix}h_i, & 0\\ L(h_i), & 1\end{pmatrix},\quad \bar{x}\to\begin{pmatrix}x, & 0\\ t_x, & 1\end{pmatrix}$$

$$\bar{h}_j\to\begin{pmatrix}h_j, & 0\\ L(h_j), & 1\end{pmatrix}$$

とすると，Hにおいて $h_ix=h_j$ が成り立つことから

(15.5.26)
$$c_{ij}\to\begin{pmatrix}h_ixh_j^{-1}, & 0\\ L(h_i)xh_j^{-1}+t_xh_j^{-1}-L(h_j)h_j^{-1}, & 1\end{pmatrix}$$
$$=\begin{pmatrix}1, & 0\\ L(h_i)h_i^{-1}+t_xh_j^{-1}-L(h_j)h_j^{-1}, & 1\end{pmatrix}$$

となる．

$\bar{h}_i$ に対応する行列に現われる線形形式 $L(h_i)$ をもっと詳細に考察する必要がある．ただし

$$\bar{x}\to\begin{pmatrix}x, & 0\\ t_x, & 1\end{pmatrix}\qquad \bar{x}^{-1}\to\begin{pmatrix}x^{-1}, & 0\\ -t_xx^{-1}, & 1\end{pmatrix}$$

である．$a=x$ が生成元のとき $q(a)=t_a$, $a^{-1}=x$ が生成元のとき $q(a)=-t_aa^{-1}$ と書くことにしよう．すると a_i を $\bar{x}, \bar{y}, \cdots$ または $\bar{x}^{-1}, \bar{y}^{-1}, \cdots$ のどれかとし，$\bar{h}=a_1a_2\cdots a_r$ を任意の語とするとき，

$$\bar{h}\to\begin{pmatrix}h, & 0\\ L(h), & 1\end{pmatrix}$$

となる．ただし，$h=a_1a_2\cdots a_r$ のとき

(15.5.27)
$$L(h)=q(a_1)a_2\cdots a_r+q(a_2)a_3\cdots a_r+\cdots$$
$$+q(a_{r-1})a_r+q(a_r)$$

である．

この公式は行列の積の規則と r についての帰納法により容易に確かめられる．さらに (15.5.27) から

(15.5.28)
$$L(h)h^{-1}=q(a_1)a_1^{-1}+q(a_2)a_2^{-1}a_1^{-1}+\cdots$$
$$+q(a_r)a_r^{-1}a_{r-1}^{-1}\cdots a_1^{-1}$$

という公式が得られることに注意する．もしhが標準形ならば$q(a_i)$は$a_1a_2\cdots a_i$の逆元をかけられているが，Wの代表元がSchreierの性質を持つから，これも標準形であることに注意する．したがって，群環H^*の基底として，Hの元の標準形の逆元を使うと便利である．

Wの各c_{ij}に対し，h_jとxが一意的に定まる．ゆえにc_{ij}に$t_xh_j^{-1}$という項を付随させることができる．h_jは標準形で，h_jx^{-1}は既約形ではあるが標準形ではなく，この項はh_iの標準形に等しいということにより特徴づけられる．しかし(15.5.26)において線形形式$L(h_i)h_i^{-1}+t_xh_j^{-1}-L(h_j)h_j^{-1}$はこの形の項はこれ以外に含んでいない．なぜなら$L(h_i)h_i^{-1}$や$L(h_j)h_j^{-1}$から出てくる他の項は(15.5.28)により$q(a_k)a_k^{-1}\cdots a_1^{-1}$という形をしていて，$a_1\cdots a_k$は$h_i$や$h_j$の最初の切口で，$h$達はSchreier条件を満たすから，それ自身あるhの標準形になる．そして，$a_k=y$が生成元とすると，$q(a_k)a_k^{-1}\cdots a_1^{-1}=t_yy^{-1}\cdots a_1^{-1}=t_yh^{-1}$となり，$h$は$y$で終るから$hy^{-1}$は既約形でない．$y$を1つの生成元とし，$a_k=y^{-1}$とすると$q(a_k)a_k^{-1}\cdots a_1^{-1}=-t_y\cdot a_{k-1}^{-1}\cdots a_1^{-1}=-t_yh^{-1}$となり，$hy^{-1}=a_1\cdots a_k$は標準形である．ゆえに，$c_{ij}$に付随する線形形式においてこの形をした項は$t_xh_j^{-1}$だけである．また異なる$c_{ij}$は異なる項をもつ．ゆえに線形形式$L(c_{ij})$は線形独立で，$c_{ij}$は自由可換群を生成し，それは$W/W'$に同型となる．ゆえに$\bar{x},\bar{y},\cdots$に対応する行列で生成される群$K$は$T=F_1/W'$の忠実な表現になり，補題が証明された．

15.6. 両側加群

Ωを乗法群，Aを**両側 Ω-加群**(double Ω-module)とする．すなわちAは加法的に書かれた可換群で次の条件を満たす．

1) ΩはAに両側から作用し，$a\in A$と$\xi\in\Omega$が与えられるとξaと$a\xi$というAの元が一意的に定まる．

2) 分配律

$$\xi(a_1+a_2)=\xi a_1+\xi a_2,\quad (a_1+a_2)\xi=a_1\xi+a_2\xi$$

が成り立つ．したがって

$$-\xi a=\xi(-a),\quad -a\xi=(-a)\xi,\quad \xi 0=0\xi=0$$

となる．

3) Ω の単位元を1とすると，$1a=a1=a$ が成り立つ．

4) 結合律 $\xi(\eta a)=(\xi\eta)a$，$(\xi a)\eta=\xi(a\eta)$ および $(a\xi)\eta=a(\xi\eta)$ が成り立つ．

これらの規則はすべての $a_1, a_2, a\in A$ およびすべての $\xi,\eta\in\Omega$ に対して成り立つ．

両側 Ω-加群というのは加法的な可換群で，$\Omega\times\Omega$ の元 (ξ,η) を分配的作用素としてもつものである．

応用上では Ω はどちらか一方，たとえば左側からは自明な方法で作用することがしばしばある．これはすべての $\xi\in\Omega$ と $a\in A$ に対し $\xi a=a$ となることを意味する．このような場合には左側からの作用を省略し，右加群とよぶ．

たとえば A をある群 G の可換正規部分群とし，$\Omega=G/A$ と置く．$\xi=Au_\xi$ とすると，$u_\xi^{-1}au_\xi$ は a と ξ にのみ関係し，剰余類の中での u_ξ の選び方には関係しない．したがって，あいまいさなしに $u_\xi^{-1}au_\xi=a^\xi$ と書くことができる．これで右加群の例が得られたわけだが，ここでは A は乗法的に書かれている．しかしコホモロジーの一般論を展開するためには A を加法的に書いた方が便利である．

15.7. コチェイン，コバウンダリとコホモロジー群*)

両側 Ω-加群 A が与えられたとき，$C^n=C^n(A,\Omega)$ を A に値をとり，Ω 上を独立に動く n 変数関数で少なくとも1つの $\xi_i=1$ ならば

(15.7.1) $$f(\xi_1,\cdots,\xi_n)=0$$

となるもの全体のつくる加法群と定義する．C^n の元は **n 次元コチェイン** (n-dimensional cochain) とよばれる．$C^0=A$ と定義する．したがって0次元コチェインというのは A の元のことである．

コバウンダリ作用素 (coboundary operator) δ は

---

*) Eilenberg-MacLane [1,2] MacLane [2] 参照

$$(15.7.2)\qquad (\delta f)(\xi_0, \xi_1, \cdots, \xi_n)=\xi_0 f(\xi_1, \cdots, \xi_n) + \sum_{=1}^{n}(-1)^t f(\xi_0, \xi_1, \cdots, \xi_{t-2}, \xi_{t-1}\xi_t, \xi_{t+1}, \cdots, \xi_n) + (-1)^{n-1} f(\xi_0, \xi_1, \cdots, \xi_{n-1})\xi_n$$

という規則により各 C^n を C^{n+1} の中に写す．$f\in C^n$ とすると $\delta f\in C^{n+1}$ となることはすぐに確かめられる．写像 $f\to\delta f$ は加法に関して準同型である．群論において実際に役に立つのは $n=0, 1, 2$ の場合だけのようである．このときのコバウンダリ作用素の公式は

$$(15.7.3)\qquad (\delta f)(\xi)=\xi f-f\xi \qquad f=a\in A$$
$$=\xi a-a\xi,$$
$$(\delta f)(\xi, \eta)=\xi f(\eta)-f(\xi\eta)+f(\xi)\eta,$$
$$(\delta f)(\xi, \eta, \zeta)=\xi f(\eta, \zeta)-f(\xi\eta, \zeta)+f(\xi, \eta\zeta)-f(\xi, \eta)\zeta$$

となる．

定理 15.7.1. 任意のコチェイン f について，$\delta^2 f=0$ が成り立つ．

証：$f\in C^{n-2}$ となる n をとる．すると $\delta f\in C^{n-1}$ となるから $(\delta^2 f)(\xi_1, \xi_2, \cdots, \xi_n)$ を定義により δf の値を使って表わすと，交代符号の $n+1$ 個の項の和，たとえば

$$u_0-u_1+u_2-\cdots+(-1)^n u_n$$

となる．各 u_i を f の値を使って表わすと，交代符号の n 個の項の和として

$$u_i=u_{i0}-u_{i1}+\cdots+(-1)^{i-1}u_{i,i-1} + (-1)^i u_{i,i+1}+\cdots+(-1)^{i+j-1}u_{i,i+j}+\cdots$$

と表わされ，i, j を1から n まで動かすと

$$\delta^2 f(\xi_1, \cdots, \xi_n)=\sum_{i<j}(-1)^{i+j-1}u_{ij}+\sum_{i>j}(-1)^{i+j}u_{ij}$$

となる．ところが任意の i, j に対し $u_{ij}=u_{ji}$ となることが容易に確かめられるから上の和は0となる．

$f\in C^n$ は $\delta f=0$ となるとき，n 次元**コサイクル**（cocycle）とよばれる．n 次元コサイクルの全体は δ によって引き起こされる C^n から C^{n+1} の中への

準同型の核 $Z^n = Z^n(A, \Omega)$ である．

$f \in C^n$ は $\delta g = f$ となる $g \in C^{n-1}$ が存在するとき n 次元コバウンダリ（coboundary）とよばれる．n 次元コバウンダリの全体は写像 δ による C^{n-1} の像 $B^n = B^n(A, \Omega)$ である．$B^0 = 0$ と定義する．

上の定理により任意のコバウンダリはコサイクルであり，すべての n に対し $B^n \subseteq Z^n$ が成り立つ．商群 Z^n/B^n は両側 Ω–加群 A の n 次元**コホモロジー群**（cohomology group）とよばれ，

$$H^n(A, \Omega) = Z^n/B^n$$

と書く．

コチェイン $f(\xi_1, \cdots, \xi_n)$ の定義において1つ以上の変数が単位元ならばコチェインの値が0となるという制限（15.7.1）をつけた．これは多くの場合，特に前に定義した因子団に応用するためには望ましい制限である．このようなコチェインは**正規化されている**（normalized）といわれる．制限（15.7.1）を除いた場合，**正規化されていないコチェイン**（unnormalized cochain）という言葉を使う．定理15.7.1では条件（15.7.1）を使っていないので，この定理はどちらの場合にも成り立つ．この区別は便宜的なもので，正規化されていないコチェインから作ったすべての次元のコホモロジー群は正規化されているコチェインから作ったものに同型であることを示そう．

定理 15.7.2. すべての次元のコホモロジー群 $H^n(A, \Omega)$ は正規化されていないコチェインに対して作ったものと，正規化されているコチェインに対して作ったものは同型である．

証：n 次元の正規化されたコチェイン，コバウンダリ，コサイクルの全体を C^n, B^n, Z^n と書き，正規されていないものをそれぞれ C'^n, B'^n, Z'^n と書こう．

$n=0$ と $n=1$ については $B^0 = B'^0 = 0$, $Z^0 = Z'^0$ および $B^1 = B'^1$, $Z^1 = Z'^1$ がすぐに確かめられ，いずれの場合にも $H^0(A, \Omega)$ と $H^1(A, \Omega)$ は同じになる．このとき一番確かめるべきことは $Z^1 = Z'^1$ であるが，$f(\xi) \in Z'^1$ ならば

$\xi f(\eta)-f(\xi\eta)+f(\xi)\eta=0$ であるから，$\xi=\eta=1$ と置けば $f(1)=0$ となり，$f(\xi)$ は正規化されている．したがって $Z'^1=Z^1$ となる．

そこで $n>1$ とする．明らかに $B^n\subseteq B'^n$, $Z^n\subseteq Z'^n$ である．したがって C^n についてのコホモロジー類，すなわち C^n における B^n の剰余類に対応する C'^n についてのコホモロジー類が一意的に定まる．すなわちそれを含む B'^n の剰余類である．この対応は明らかに $H^n(A,\Omega)$ から $H'^n(A,\Omega)$ の中への準同型である．同型であることを証明するためにはこの対応が一対一であることをいわなければならないが，それには次の2つの補題がいえればよい．2つのコチェインはその差がコバウンダリであるとき**コホモロガス**（cohomologous）であるという．特に2つのコサイクルは同じコホモロジー類に属すとき，コホモロガスである．

補題 15.7.1. 任意の正規化されていないコサイクルはある正規化されたコサイクルとコホモロガスである．

補題 15.7.2. あるコチェインのコバウンダリが正規化されていれば，それは正規化されたコチェインのコバウンダリである．

補題の証：コチェイン $f(x_1,\cdots,x_n)$ は，最初の i 変数のうちの1つが単位元ならば0となるとき，i 番目まで正規化されている，または簡単に i-正規ということにしよう．0-正規なコチェインの全体というのは正規化されていないコチェインの全体 C'^n で，n-正規なコチェインの全体というのは正規化されたコチェインの全体 C^n である．$f(x_1,\cdots,x_n)$ に対し，$f=f_0$ と定義し，あとは帰納的に

$$f_{i+1}=f_i-\delta g_{i+1}\qquad i=0,\cdots,n-1 \tag{15.7.4}$$

によりコチェイン f_{i+1} を定義する．ただし

$$g_{i+1}(x_1,\cdots,x_{n-1})=(-1)^i f_i(x_1,\cdots,x_i,1,x_{i+1},\cdots,x_{n-1}) \tag{15.7.5}$$

である．$f=f_0$ と f_n の差はコバウンダリで，$f=f_0,f_1,\cdots,f_n$ について $\delta f_i=\delta f_{i+1}$ であるから，これらのコバウンダリはすべて同じで δf であることを

注意しておく．

補題 15.7.3. δf が正規化されていれば，f_i は i-正規である．

この補題から前の2つの補題が証明される．補題15.7.1については，f を正規化されていないコサイクルとすると $\delta f=0$ で，これは明らかに正規化されているから，f_n は正規化されているコサイクルで，$f_0=f$ とコホモロガスである．補題15.7.2については，$g=\delta f$ がコバウンダリで正規化されていれば，たとえば $g\in C^{n+1}$ とすると，$g=\delta f_0=\cdots=\delta f_n$ で f_n は正規化されている．

補題15.7.3を i に関する帰納法で証明することにしよう．$i=0$ のときは明らかに成り立っている．そこで，i までは正しいとして，$i+1$ のときを考えよう．

$$f_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)=0 \tag{15.7.6}$$

を証明することが必要だが，(15.7.4) における f_{i+1} の定義から

$$\begin{aligned}
f_{i+1}&(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&=f_i(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&\quad -x_1 g_{i+1}(x_2, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&\quad +\sum_{j=1}^{i-1}(-1)^{j-1}g_{i+1}(x_1, \cdots, x_jx_{j+1}, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)\\
&\quad +(-1)^{i-1}g_{i+1}(x_1, \cdots, x_{i-1}, x_i\cdot 1, x_{i+2}, \cdots, x_n)\\
&\quad +(-1)^{i}g_{i+1}(x_1, \cdots, x_i, 1\cdot x_{i+2}, \cdots, x_n)\\
&\quad +\sum_{j=i+2}^{n-1}(-1)^{j-1}g_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_jx_{j+1}, \cdots, x_n)\\
&\quad +(-1)^{n-1}g_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_{n-1})x_n
\end{aligned} \tag{15.7.7}$$

となる．帰納法の仮定より f_i は i-正規であるから，(15.7.5) より g_{i+1} も i-正規である．したがって (15.7.7) において，x_1 が左についた項と，$j=1$ から $i-1$ までの和はすべて0であることが分かる．そしてその次の2つの項は互いに消し合っている．そこで残った項について，g_{i+1} をその定義 (15.7.5) に従って置き換えると (15.7.7) は

$$f_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n) \tag{15.7.8}$$

$$=f_i(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)$$
$$+\sum_{j=i+2}^{n-1}(-1)^{i+j-1}f_i(x_1, \cdots, x_i, 1, 1, x_{i+2}, \cdots, x_jx_{j+1}, \cdots, x_n)$$
$$+(-1)^{n+i-1}f_i(x_1, \cdots, x_i, 1, 1, x_{i+2}, \cdots, x_{n-1})x_n$$

となる．ところが $\delta f_i=\delta f$ は正規化されていると仮定したから，

(15.7.9)　$$(-1)^{i+1}\delta f_i(x_1, \cdots, x_i, 1, 1, x_{i+2}, \cdots, x_n)=0$$

で，帰納法の仮定により，f_i は i-正規であるから，(15.7.8) の右辺は (15.7.9) を展開したときに消えない項全体から成っている．ゆえに

(15.7.10)　$$f_{i+1}(x_1, \cdots, x_i, 1, x_{i+2}, \cdots, x_n)=0$$

となり，帰納法により補題15.7.3が証明され，補題15.7.1と補題15.7.2，それに定理が順番に証明されたわけである．

15.8. 拡大理論へのコホモロジーの応用

A を群 G の可換正規部分群とし，$\Omega=G/A$ をその商群とする．剰余類 $Au_\xi=\xi$ を Ω の元とするとき，$a\in A$ に対して $u_\xi^{-1}au_\xi$ は a と ξ にのみ関係し，剰余類の中での u_ξ の選び方にはよらない．したがって，あいまいさなしに $u_\xi^{-1}au_\xi=a\xi$ と書くことができ，このようにして，Ω は A の右からの作用素から成る群となる．また Ω は左からは自明な作用をしていると考え，A は加法的に書くことにする．ある因子団の因子を $f(u, v)=(u, v)$ と書くことにすると，(15.2.2) は

(15.8.1)　$$f(uv, w)+f(u, v)w=f(u, vw)+f(v, w)$$

となる．項を並べかえると，

(15.8.2)　$$f(v, w)-f(uv, w)+f(u, vw)-f(u, v)w=0$$

となり，因子団というのは2次元のコサイクルであることがわかる．2つの因子団 $f(u,v)$ と $f_1(u, v)$ が同値であるための条件 (15.2.3) は

(15.8.3)　$$f_1(u, v)=f(u, v)+\alpha(v)-\alpha(uv)+\alpha(u)v,$$

すなわち f_1 と f の差がコバウンダリ $\alpha(v)-\alpha(uv)+\alpha(u)v$ である．ここで Ω の左からの作用は自明な作用であることに注意する．したがって，拡大の群と

いうのは2次元のコホモロジー群 $H^2(A,\Omega)$ と一致する．このことを定理の形で述べておくことにする．

定理 15.8.1. 可換群 A の群 Ω による拡大の群は2次元のコホモロジー群 $H^2(A,\Omega)$ である．ただし

1) Ω は A に左からは自明に働く．

2) 右からの作用は A の自己同型を引き起こす．

3) 因子団 $f(u,v)$ はコサイクルの全体 Z^2 である．

4) 同値な因子団の差は B^2 にはいるコバウンダリである．

G を A による剰余類の和として表わすときに，A の代表元として単位元を選ぶことにより，$f(1,1)=0$ と正規化される．(15.8.1) において $u=v=1$ と置くと，

(15.8.4) $$f(1,w)+f(1,1)w=f(1,w)+f(1,w).$$

したがって

(15.8.5) $$f(1,w)=0$$

となる．同様に $v=w=1$ と置くと

(15.8.6) $$f(1,1)-f(u,1)+f(u,1)-f(u,1)=0,$$

したがって

(15.8.7) $$f(u,1)=0$$

となり，我々の扱っているのは正規化されたコサイクルである．

定理 15.2.1 を特別な場合として含むようなコホモロジーの一般的定理を証明することにしよう．

Ω は有限位数 m としよう．すると各 $n>0$ に対して

(15.8.8) $$(\sigma f)(x_2,\cdots,x_n)=\sum_{x\in\Omega}x^{-1}f(x,x_2,\cdots,x_n)$$

という公式により，C^n を C^{n-1} の中に写す加法的準同型 σ が定義できる．$f\in C^n$ とすると，$\sigma f\in C^{n-1}$ となることは明らかである．

$g=\sigma f$ と置き $(\delta g)(x_1,\cdots,x_n)$ を計算しよう．

(15.8.9) $$\delta g(x_1,\cdots,x_n)$$

$$
\begin{aligned}
&= x_1 \sum x^{-1} f(x, x_2, \cdots, x_n) \\
&\quad - \sum x^{-1} f(x, x_1 x_2, \cdots, x_n) \\
&\qquad \cdots\cdots\cdots\cdots\cdots\cdots \\
&\quad + (-1)^{j-1} \sum x^{-1} f(x, x_1, \cdots, x_{j-1} x_j, \cdots, x_n) \\
&\qquad \cdots\cdots\cdots\cdots\cdots\cdots \\
&\quad + (-1)^{n-1} \sum x^{-1} f(x, x_1, \cdots, x_{n-1} x_n) \\
&\quad + (-1)^n [\sum x^{-1} f(x, x_1, \cdots, x_{n-1})] x_n.
\end{aligned}
$$

ここでの $\sum$ はすべての $x \in \Omega$ についての和である.

次に $(\delta f)(x, x_1, \cdots, x_n)$ を考えよう.

$$
\begin{aligned}
(15.8.10) \qquad & (\delta f)(x, x_1, \cdots, x_n) \\
&= x f(x_1, \cdots, x_n) \\
&\quad - f(x x_1, x_2, \cdots, x_n) \\
&\quad + f(x, x_1 x_2, \cdots, x_n) \\
&\qquad \cdots\cdots\cdots\cdots\cdots\cdots \\
&\quad + (-1)^n f(x, x_1, \cdots, x_{n-1} x_n) \\
&\quad + (-1)^{n+1} f(x, x_1, \cdots, x_{n-1}) x_n.
\end{aligned}
$$

(15.8.10) を使うと,

$$
\begin{aligned}
(15.8.11) \qquad & \sigma(\delta f)(x_1, \cdots, x_n) \\
&= \sum_{x \in \Omega} x^{-1} (\delta f)(x, x_1, \cdots, x_n) \\
&= m f(x_1, \cdots, x_n) \\
&\quad - \sum x^{-1} f(x x_1, x_2, \cdots, x_n) \\
&\quad + \sum x^{-1} f(x, x_1 x_2, \cdots, x_n) \\
&\qquad \cdots\cdots\cdots\cdots\cdots\cdots \\
&\quad + (-1)^n \sum x^{-1} f(x, x_1, \cdots, x_{n-1} x_n) \\
&\quad + (-1)^{n+1} \sum x^{-1} f(x, x_1, \cdots, x_{n-1}) x_n.
\end{aligned}
$$

和 $S = \sum_{x \in \Omega} x^{-1} f(x x_1, x_2, \cdots, x_n)$ において, $y = x x_1$ と置き, x_1 を Ω の固定した元とすると, x が Ω 全体を動くとき, y も Ω 全体を動くから,

$$
S = x_1 \sum y^{-1} f(y, x_2, \cdots, x_n) = x_1 \sigma f(x_2, \cdots, x_n)
$$

となる．ゆえに (15.8.11) は

(15.8.12) $$(\sigma(\delta f))=mf-\delta(\sigma f)$$

となる．

定理 15.8.2. $f\in C^n$ ならば $\sigma(\delta f)+\delta(\sigma f)=mf$ が成り立つ．

系 15.8.1. $f\in Z^n$ ならば $mf\in B^n$ となる．

なぜなら，$f\in Z^n$ ならば $\delta f=0$ で，したがって mf は σf のコバウンダリとなる．結局 Ω の位数が m ならばコホモロジー群 $H^n=Z^n/B^n$ の任意の元の位数は m を割り切ることが分かった．定理 15.2.1 は $n=2$ の場合になっている．

因子団に関してはさらに Gaschütz [1] によって与えられた定理がある．ただしもっと一般的な形では Eckmann [1] によって与えられた．これは群 Ω のコホモロジーと部分群 B のコホモロジーとを関係づけるものである．B の Ω における指数 m は有限だとする．

(15.8.13) $$\Omega=B\cdot 1+Bs_2+\cdots+Bs_m,\ s_1=1.$$

ただし，$a_1, a_2, \cdots, a_n$ を Ω の元として，$\overline{s_ia_1}=s_{i1}$ と書くことにする．ただし上に線を引くのは剰余類の代表元を意味する．また，

$$\overline{s_{i1}a_2}=s_{i2},\ \cdots,\ \overline{s_{in-1}a_n}=s_{in}$$

と置く．$f(a_1, \cdots, a_n)\in C^n$ の**移送** (transfer) $T(f(a_1, \cdots, a_n))$ を

(15.8.14) $$T(f(a_1, \cdots, a_n))$$
$$=\sum_{i=1}^m s_i^{-1}f(s_ia_1s_{i1}^{-1}, s_{i1}a_2s_{i2}^{-1}, \cdots, s_{in-1}a_ns_{in}^{-1})s_{in}$$

によって定義する．常に $s_{ij-1}a_js_{ij}^{-1}\in B$ で，$f\in C^n(A, \Omega)$ に対して，Tf は部分群 $\Omega C^n(A, B)\Omega$ にはいることに注意する．

定理 15.8.3. **(Gaschütz の定理)** $f(a_1, \cdots, a_n)\in Z^n$ で，B が Ω の指数 m の部分群ならば，

$$Tf(a_1, \cdots, a_n)\equiv mf(a_1, \cdots, a_n) \bmod B^n$$

が成り立つ．

系 15.8.2. 移送のコホモロジー類は（15.8.13）における剰余類の代表系 s_i の選び方には関係しない．

定理の証：

(15.8.15)
$$\sum_{i=1}^{m}(\delta f)(s_i^{-1}, s_ia_1s_{i1}^{-1}, \cdots, s_{in-1}a_ns_{in}^{-1})s_{in}$$
$$-\sum_{i=1}^{m}(\delta f)(a_1, s_{i1}^{-1}, s_{i1}a_2s_{i2}^{-1}, \cdots, s_{in-1}a_ns_{in}^{-1})s_{in}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$+(-1)^{j-1}\sum_{i=1}^{m}(\delta f)(a_1, \cdots, a_{j-1}, s_{ij-1}^{-1}, s_{ij-1}a_js_{ij}^{-1}, \cdots)s_{in}$$
$$+(-1)^{j}\sum_{i=1}^{m}(\delta f)(a_1, \cdots, a_{j-1}, a_j, s_{ij}^{-1}, s_{ij}a_{j+1}s_{ij+1}^{-1}, \cdots)s_{in}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$+(-1)^{n}\sum_{i=1}^{m}(\delta f)(a_1, \cdots, a_n, s_{in}^{-1})s_{in}=0$$

を考えよう．$f\in Z^n$ だから $\delta f=0$ で，上の各項は0である．上の $n+1$ 個の各行のコバウンダリを展開し，$i=1$ から m について加えるとどうなるか考えてみよう．第1行の第1項は

(15.8.16)
$$\sum s_i^{-1}f(s_ia_1s_{i1}^{-1}, \cdots, s_{in-1}a_ns_{in}^{-1})s_{in}=Tf(a_1, \cdots, a_n)$$

となる．最後の行の最後の項は

(15.8.17)
$$(-1)^n(-1)^{n+1}\sum f(a_1, \cdots, a_n)s_{in}^{-1}\cdot s_{in}$$
$$=-mf(a_1, \cdots, a_n)$$

となる．$s_{ij-1}^{-1}\cdot s_{ij-1}a_js_{ij}^{-1}=a_j\cdot s_{ij}^{-1}$ であるから，$j=1, \cdots, n$ について第 j 行と第 $j+1$ 行の（$j+1$）番目の項は互いに消し合う．そこで，第（$j+1$）行の最初の j 項と，第 j 行の $j+2, \cdots, n+2$ 番目の項を一緒にして考えよう．これらは

(15.8.18)
$$(-1)^ja_1\sum_{i=1}^{m}f(a_2, \cdots, a_j, s_{ij}^{-1}, s_{ij}a_{j+1}s_{ij+1}^{-1}, \cdots)s_{in}$$
$$(-1)^{j+1}\sum_{i=1}^{m}f(a_1a_2, \cdots, a_j, s_{ij}^{-1}, s_{ij}a_{j+1}s_{ij+1}^{-1}, \cdots)s_{in}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(-1)^{2j}\sum_{i=1}^{m} f(a_1, \cdots, a_{j-1}a_j, s_{ij}{}^{-1}, s_{ij}a_{j+1}s_{ij+1}{}^{-1}, \cdots)s_{in}$$

$$(-1)^{2j+1}\sum_{i=1}^{m} f(a_1, \cdots, a_{j-1}, s_{ij-1}{}^{-1}, a_ja_{j+1}s_{ij}{}^{-1}, \cdots)s_{in}$$

…………………………………………………………

$$(-1)^{n+j+1}\sum_{i=1}^{m} f(a_1, \cdots, a_{j-1}, s_{ij-1}{}^{-1}, s_{ij-1}a_js_{ij}{}^{-1}, \cdots)s_{in-1}a_n$$

である．そこで $u_1, \cdots, u_{n-1}$ を変数とする関数 $F_j(u_1, \cdots, u_{n-1})\in C^{n-1}$ を

(15.8.19)　$F_j(u_1, \cdots, u_{n-1})$

$$= \sum_{i=1}^{m} f(u_1, \cdots, u_{j-1}, \sigma_i{}^{-1}, \sigma_iu_j\sigma_{ij}{}^{-1}, \cdots, \sigma_{in-1}u_{n-1}\sigma_{in}{}^{-1})\sigma_{in}$$

によって定義する．ただし，$\sigma_i=s_i$ で $\sigma_{it}=\overline{\sigma_{it-1}u_t}$ と帰納的に定義する．すると (15.8.18) の項はコバウンダリ $(-1)^j(\delta F_j)(a_1, \cdots, a_n)$ であることが分かる．なぜなら，i について加えるとき s_{ij} や s_{ij-1} は σ_i と同じ働きをするからである．j を1から n まで動かすと，コバウンダリ $(-1)^j(\delta F_j)(a_1, \cdots, a_n)$ は (15.8.15) の項のうち，互いに消し合うものと，(15.8.16)，(15.8.17) 以外のすべての項を尽し，定理が証明される．

Gaschütz の定理を群論的な形で述べると次のようになる；

定理 15.8.4. (**Gaschütz の定理**) 可換群 A の有限群 H による1つの H-χ 拡大の因子団を $F=[(u, v)]$, $u, v\in H$, $(u, v)\in A$ とする．B を H の指数 m の部分群，

$$H=B\cdot 1+Bs_2+\cdots+Bs_m,\quad s_1=1$$

とすると，

$$(u, v)^m\sim \prod_{i=1}^{m}(s_iu\overline{s_iu}^{-1}, \overline{s_iu}v\overline{s_iuv}^{-1})^{\overline{s_iuv}}$$

となる．変数 $s_iu\overline{s_iu}^{-1}, \overline{s_iu}v\overline{s_iuv}^{-1}$ は B の元である．

系 15.8.3. $x, y\in B$ ならば $(x, y)=1$ が成り立っているとすると，$(u, v)^m\sim 1$ となる．

この定理からいろいろのことが導かれるが，特に A の H-χ 拡大と A の

$S(p)-\chi$ 拡大とを関係づける方法が非常に有用である．ただし，$S(p)$ はHのSylow p-部分群である．H の位数を $n=p^e m, S(p)$ の位数を p^e とする．$E=E(H)$ を§15.2で定義したAの $H-\chi$ 拡大の群とする．Eの各元は同値な因子団 $F_i=[(u,v)_i]$ の類である．定理15.2.1により，E の各元の位数は nを割り切る．したがって，Eは周期的可換群で，その Sylow 部分群 $E(p)$ の直積となる．

定理 15.8.5. 可換群 A の有限群 H による $H-\chi$ 拡大の群 $E=E(H)$ の Sylow p-部分群 $E(p)$ は，$S(p)$ をHの Sylow p-部分群とするとき，Aの $H-\chi$ 拡大の因子団 $F=[(u,v)]$ の変数を $(x,y), x, y\in S(p)$ に制限して得られる $S(p)-\chi$ 拡大の群 E_p に同型である．

証：Aの $H-\chi$ 拡大の因子団 $F=[(u,v)]$ 上に p-同値関係

$$(u,v)\underset{p}{\sim}(u,v)_1$$

を，変数を $x, y\in S(p)$ に制限して得られる $S(p)-\chi$ 拡大について

$$(x,y)\sim(x,y)_1$$

となることを定義する．これが実際に同値関係となることはすぐに分かる．さらに，x, y を $S(p)$ に制限したとき，$(x,y)\sim 1$ となる因子団 $F=[(u,v)]$ のつくるEの部分群を E_1 と置く．すると，Eの元が p-同値になるのは E_1 の同じ剰余類にはいるとき，またそのときに限る．よって E/E_1 は因子団 $F[(u,v)]$ の変数を $x, y\in S(p)$ に制限して得られる $S(p)-\chi$ 拡大の群 E_p に同型となる．Gaschütz の定理の系において部分群 B として $S(p)$ をとると，E_1 の任意の元の位数は $S(p)$ の指数を割り切り，定理15.2.1により E_p の任意の元の位数は p^e を割り切る．$(p^e, m)=1$ であるから，E_p と，Eの Sylow p-部分群 $E(p)$ は E/E_1 に同型となる．よってこの2つの群が同型となり，定理が証明された．

定理 15.8.6. Aの $H-\chi$ 拡大がA上分解するためには，Hの位数を割る各素数 p について，この拡大を H のある Sylow p-部分群 $S(p)$ に制限したと

き，分解することが必要十分である．

証：H が A 上分解すれば，$S(p)$ が A 上分解することは明らかである．逆を証明しなければならない．$F=[(u,v)]$ を $H-\chi$ 拡大を決める因子団とする．仮定より $(u,v)\sim(u,v)_1$ で $x,y\in S(p)$ については $(x,y)_1=1$ である．$n=p^e m$ とすると，系より $(u,v)^m\sim(u,v)_1{}^m\sim1$ となる．そして，これは n を割るすべての p に対して起こらなければならない．$(u,v)^m\sim1$ となる m の最大公約数は 1 だから $(u,v)\sim1$ となり，H は A 上分解する．よって定理が証明された．

第16章 群の表現

16.1. 一般的注意

群Gから群Wへの準同型αを群Gの**表現**（representation）という．価値のあるのは計算の役に立つ群WによるGの表現である．たとえば，第5章で論じた群Gの置換表現というのは，Gから対称群S_nの中への準同型のことである．

対称群の代りに，体F上のベクトル空間Vの自己準同型[1]の全体によって表現することもできる．自己準同型のうち一対一のもの[2]全体は群をつくり，VがF上有限次元nのとき，この群はn次**全線形群**（full linear group）$L_n(F)$[3]とよばれ，F上の正則$n\times n$行列で表わされる．これは線形変換によるGの表現を考えることである．このとき，Gの元はVに作用していると考えることができる．したがって，Gに対応する線形変換で自分自身の中に写されるVの部分空間というのは，表現の不変部分空間のことであって，VをFとGを作用素としてもつ加法群とみたときの認容部分群Nになっている．

ベクトル空間Vの自己準同型の全体は環をつくっている．したがって，GのV上の線形表現から加法とスカラー乗法により，GのF上の群環R_Gの線形表現が得られ，Vの任意の認容部分群NはGの表現だけでなく，R_Gの表現も与える．ゆえに，群環R_Gの分解と線形表現の分解との間に密接な関係があることも，驚くには当たらないであろう．しかし，歴史的には，群の表現論と環の構造論とは別々に発展してきたのであって，これらの密接な関係が認識される

---

1) VからVへの線形写像のこと．

2) つまり，Vの自己同型である．

3) 一般線形群（general linear group）ともよばれ，$GL(n, F)$または$GL_n(F)$と書かれることが多い．

ようになったのは，かなり最近のことである．

16.2. 行列表現．指標*)

定　義：群 G の n 次の行列表現というのは，G 上で定義され，全線形群 $L_n(F)$（F は何かある体）に値をとる関数 ρ で，すべての $x, y \in G$ に対して $\rho(xy)=\rho(x)\rho(y)$ を満たすもののことである．

このように定義すると，$\rho(x)$ は正則行列で，$x \to \rho(x)$ は G から $L_n(F)$ への準同型となることに注意する．$\rho(1)=I_n$（$n\times n$ 単位行列），$\rho(x^{-1})=[\rho(x)]^{-1}$（$\rho(x)$ の逆行列）となる．準同型 $x\to\rho(x)$ の核 K は G の正規部分群で，行列 $\rho(x)$ は G/K を忠実に表現する．表現が忠実となるのは，核 K が 1 のときである．

定　義：表現 ρ の指標 χ というのは，$\chi(x)=\mathrm{trace}\,\rho(x)$ により定義された G 上の関数のことである．

したがって，指標のとる値は体 F の数である．1 次の表現については $\chi=\rho$ が成り立つ．

2 つの表現 ρ と ρ^* は，任意の $x\in G$ について $\rho^*(x)=S^{-1}\rho(x)\,S$ が成り立つような正則行列 $S\in L_n(F)$ が存在するとき**同値**（equivalent）であるという．逆に，S を $L_n(F)$ の任意の正則行列，$\rho(x)$ を $L_n(F)$ における表現とすると，$S^{-1}\rho(x)S=\rho^*(x)$ も表現となることに注意する．実際，$\rho(x), x\in G$ を F 上のベクトル空間 V からそれ自身への基底 $u_1, \cdots, u_n$ に関する線形変換から成る群とみたとき，

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = S \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

とすると，$S^{-1}\rho(x)S=\rho^*(x)$，$x\in G$ も同じ線形変換のつくる群で，基底 v_1,

*) 行列，行列式，全線形群の性質のうち，ここで仮定されているものについては，Birkhoff-MacLane [1] の第VI章から第IX章までに書かれている．

$\cdots, v_n$ に関して表わしたものである．

補題 16.2.1. 指標は類関数である．すなわち，共役な元の指標は一致する．

補題 16.2.2. 同値な表現の指標は一致する．

n 次行列Aの固有多項式は，$f(\lambda)=|A-\lambda I|=(-1)^n[\lambda^n-a_1\lambda^{n-1}\cdots+(-1)^n a_n]$ と定義される．ただし，係数 $a_1=\mathrm{trace}(A)$, $a_n=|A|$（Aの行列式）である．T が正則行列ならば，$|T^{-1}AT-\lambda I|=|T^{-1}(A-\lambda I)T|=|T^{-1}|\cdot|A-\lambda I|\cdot|T|=|A-\lambda I|$ となる．したがって，A と $T^{-1}AT$ は同じ固有多項式をもち，特にトレースは等しい．したがって，$\rho(y^{-1}xy)=\rho(y)^{-1}\rho(x)\rho(y)$ と $\rho(x)$ のトレースは等しく，$\chi(y^{-1}xy)=\chi(x)$ は類関数である．同様にして，$\rho^*(x)=S^{-1}\rho(x)S$ と $\rho(x)$ のトレースは等しく，同値な表現の指標は一致する．

ベクトル空間（または線形空間）の定義を復習しておこう．体F上のベクトル空間Vというのは次の規則によって与えられる．

V には $\alpha, \beta\in V$ に対して **2項加法**（binary addition）$\alpha+\beta\in V$, および $c\in F$, $\alpha\in V$ に対して**スカラー倍**（scalar product）$c\alpha$ が定義されていて，次の条件を満たす．

V1）Vは加法に関し可換群をつくる．

V2）$c(\alpha+\beta)=c\alpha+c\beta$, $(c+c')\alpha=c\alpha+c'\alpha$.

V3）$(cc')\alpha=c(c'\alpha)$；$1\alpha=\alpha$.

ただし，$\alpha, \beta\in V$, $c, c'\in F$ で，1はFの単位元である．

Vのベクトル $u_1, \cdots u_r$ は

$$a_1u_1+\cdots+a_ru_r=0,\quad a_i\in F$$

ならば，$a_1=\cdots=a_r=0$ となるとき，**線形独立**（linearly independent）であるという．さらに，$u_1, \cdots, u_n$ が線形独立で，任意の $u\in V$ が

$$u=b_1u_1+\cdots+b_nu_n,\quad b_i\in F$$

と表わせるとき，V の**基底**（basis）という．もしVが基底をもてば，どの基底も同数の元をもち，この数はベクトル空間Vの**次元**（dimension）とよばれる．

F–G **加群** (F–G module) M というのは，G が作用する F 上のベクトル空間 V で，以下の規則を満たすものと定義する．

1) $(u+v)g=ug+vg$, $u, v\in V$, $g\in G$.

2) $u(g_1g_2)=(ug_1)g_2$, $u\in V$, $g_1, g_2\in G$.

3) $u\cdot 1=u$, $u\in V$, 1 は G の単位元.

4) $(au)g=a(ug)$, $a\in F$, $u\in V$, $g\in G$.

M は G の**表現加群** (representation module) ともよばれる．

ある F–G 加群 M_1 から別の F–G 加群 M_2 への**作用準同型** (operator homomorphism) というのは，写像 $M_1\to M_2$ で次の条件を満たすもののことである．

1) $u_1\to v_1$, $u_2\to v_2$ ならば，$u_1+u_2\to v_1+v_2$.

2) $u\to v$, $b\in F$ ならば，$bu\to bv$.

3) $u\to v$, $g\in G$ ならば，$ug\to vg$.

M_1 と M_2 の**作用同型** (operator isomorphism) というのは，M_1 から M_2 の上への一対一作用準同型のことである．

M を F–G 加群，$u_1, \cdots, u_n$ を F 上の基底とし，$x\in G$ に対し写像 $v\to vx$, $v\in V$ をとったとき，$u_i\to u_ix=\sum_{j=1}^{n} a_{ij}u_j$, $i=1, \cdots, n$ とすると，$\rho(x)=(a_{ij})$, $i, j=1, \cdots, n$ は G の M における表現となる．逆に，ρ を基底 $u_1, \cdots, u_n$ をもつベクトル空間 V 上の G の表現とし，$\rho(x)=(a_{ij})=[a_{ij}(x)]$ とすると，各 $x\in G$ に対し

$$u_ix=\sum_{j=1}^{n} a_{ij}(x)u_j,\quad i=1, \cdots, n$$

と置けば，$\rho(1)=I_n$ で，$\rho(xy)=\rho(x)\rho(y)$ となるから，この規則により V は F–G 加群 M となる．したがって，n 次元の F–G 加群は G の n 次の表現を定め，逆も成り立つ．

定理 16.2.1. 2つの F–G 加群 M_1, M_2 が G の同値な表現を与えるためには，M_1 と M_2 が作用同型であることが必要十分である．

証：Gの２つの同値な表現 $\rho(x)$, $x\in G$ および $S^{-1}\rho(x)\ S$ が与えられたとする．$\rho(x)=[a_{ij}(x)]$, $x\in G$ とすると，これはGが作用しているベクトル空間Vの１つの基底 $u_1, \cdots, u_n$ と写像 $u_i\to u_i x=\sum a_{ij}(x)u_j$ に対応する．写像

$$w\to wx,\ \ w\in V$$

は

$$\begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}=S\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$

なる基底 $v_1, \cdots, v_n$ に関する表現 $\rho^*(x)=S^{-1}\rho(x)S$, $x\in G$ に対応することはすでに分かっていた．$S=(s_{ij})$ とすると，同値な表現 $\rho(x)$ と $\rho^*(x)$ は $u_i\to\sum_j s_{ij}v_j$, $i=1, \cdots, n$ によって定まる写像により作用同型となる．逆に，２つのF-G 加群 M_1 と M_2 とが作用同型だとすると，特にベクトル空間としても同型であるから，M_1 と M_2 の基底の元の数は等しい．そこで M_1 の１つの基底を $u_1, \cdots, u_n$ とすると，この作用同型により $u_1, \cdots, u_n$ は M_2 のある基底 $v_1, \cdots, v_n$ の上に写される．したがって，この作用同型により $u_i\to v_i$ だから，$u_i x\to v_i x$ となり，

$$u_i x=\sum_{j=1}^{n} a_{ij}(x)u_j,\ \ i=1, \cdots, n$$

とすると，

$$v_i x=\sum_{j=1}^{n} a_{ij}(x)v_j,\ \ i=1, \cdots, n$$

でなければならないから，M_1 と M_2 から同じ表現が得られる．ゆえに，同値な表現 $\rho(x)$ と $\rho^*(x)$ は表現加群の作用同型とちょうど対応している．

16.3. 完全可約性の定理

表現加群Mの部分加群 M_1 も表現加群になっていたとしよう．M_1 の１つの基底 $u_1, \cdots, u_r$ をとり，それに $u_{r+1}, \cdots, u_n$ をつけ加えてMの基底を完成しよう．このとき対応する表現 ρ は**可約** (reducible) であるといわれ，基底 $u_1, \cdots, u_n$ に関して，

$$\rho(x)=\left(\begin{array}{c|c} \sigma(x) & 0 \\ \hline \theta(x) & \tau(x) \end{array}\right)$$

という形をとる．ここでσとτはそれぞれr次と$n-r$次のGの表現である．表現σは基底$u_1, \cdots, u_r$を持つF-G加群M_1に付随するものであるが，τについてはどうだろうか？ これは商加群M/M_1の基底$M_1+u_{r+1}, \cdots, M_1+u_n$によって定義される表現である．もっと一般に

$$0=M_0\subset M_1\subset M_2\subset\cdots\subset M_k=M$$

を部分加群の鎖とし，Mの基底をこの鎖に適合するように選ぶと，対応する表現ρは，

$$\rho(x)=\left(\begin{array}{c|c|c|c} \rho_1(x) & & & 0 \\ \hline & \rho_2(x) & & \\ \hline & & \ddots & \\ \hline * & & & \rho_k(x) \end{array}\right)$$

という形をとり，$\rho_i(x)$はM_i/M_{i-1}の適当な基底，すなわち，u_jとしてM_iにははいるがM_{i-1}にははいらないような基底の元を動かしたときの$M_{i-1}+u_j$をとったときの表現に対応する．指標に関しては，明らかに

$$\chi(x)=\chi_1(\chi)+\chi_2(x)+\cdots+\chi_k(x)$$

が成り立つ．鎖を**極大**（maximal）にとっておけば，すなわちこれ以上細分できないようにとっておけば，M_i/M_{i-1}は真表現部分加群を持たず，**既約表現**（irreducible representation）ρ_iを与える．次のことが直ちにわかる．

補題 16.3.1. 任意の指標は既約指標の和である．

補題 16.3.2. 既約成分ρ_iは順序と作用同型を除いて一意的に定まる．

補題16.3.2は Jordan-Hölder の定理から導かれる．

表現加群Mが表現加群となる部分加群M_1を持つとき，Mが$M=M_1\oplus M_2$と直和に表わされるようなMの表現部分加群M_2が存在することがある．この場合M_2は明らかにM/M_1に作用同型で，表現$\rho(x)$は

$$\rho(x)=\left(\begin{array}{c|c} \rho_1(x) & 0 \\ \hline 0 & \rho_2(x) \end{array}\right)$$

という形をとる．逆に表現 $\rho(x)$ が主対角線上に正方行列がならぶという上のような形にできれば，M は表現部分加群 M_1 と M_2 の直和となる．この場合表現は**完全に約された**（completely reduced）という．可約な表現はすべて完全可約というわけではない．たとえば元 b で生成される無限巡回群の表現

$$\rho(b^i)=\begin{pmatrix}1, & 0\\ i, & 1\end{pmatrix}$$

は可約であるが，もし完全可約とすると，$\rho_1(b^i)$ も $\rho_2(b^i)$ も単位行列だから，すべての元が単位行列で表わされなければならない．しかし $\rho(b)=\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}$ は単位行列と共役ではないからこのようなことは起こらない．しかし次の定理に示されるように可約ならば，完全可約になるという重要な表現がある．

定理 16.3.1.（完全可約性の定理） 有限群 G の体 F 上の可約な表現は，体の標数が G の位数を割らないとき，完全可約である．

証：M を G の F 上の表現加群とし，M_1 を表現部分加群とする．$w_1, \cdots, w_r$ を M_1 の基底とし，これに $w_{r+1}, \cdots, w_n$ をつけ加えて M の基底を完成する．$w_{r+1}, \cdots, w_n$ は部分空間 N の基底とする．N は一般には表現加群とはならない．$x\in G$ に対し

$$\rho(x)=\left(\begin{array}{c|c}\sigma(x) & 0\\ \hline \theta(x) & \tau(x)\end{array}\right)$$

という形になる．また $M=M_1+N$ で，$u\in M$ は

$$u=u_1+v,\quad u_1\in M_1,\quad v\in N$$

と一意的に書ける．写像 $\eta: u\rightarrow v$ は巾等で線形である．G の位数を g とし

$$u'=\frac{1}{g}\sum_{x\in G}ux\eta x^{-1}=u\zeta$$

と置く．$u\rightarrow u'=u\zeta$ は線形写像である．この写像が定義できるためには，G の位数 g で割ることができなければならないが，G の位数 g が有限で，F の標数で割れないと仮定したから可能である．

$y\in G$ のとき，$x\in G$ に対し $z=y^{-1}x$ と置くと，x が G 全体を動くとき，z

もG全体を動くから，

$$(u\zeta)y=\frac{1}{g}\sum_x ux\eta x^{-1}y=\frac{1}{g}\sum_z (uy)z\eta z^{-1}=(uy)\zeta$$

となる．これは$M_2=M\zeta$が表現加群であることを示している．$M=M_1\oplus M_2$となることを示したい．それには任意の$u\in M$が$u=u_1+u_2, u_1\in M_1, u_2\in M_2$という形に書け，しかもこの表わし方が一意的である，すなわち$0=u_1+u_2$ならば$u_1=0=u_2$となることを示さなければならない．任意の$u\in M$に対し

$$u=(u-u\zeta)+u\zeta$$

と書くと，$u\zeta=u_2\in M_2$である．$uxu^{-1}=u$より$u-u\zeta=\frac{1}{g}\sum_x (ux-ux\eta)x^{-1}$となる．ところが$ux-ux\eta=(ux)_1\in M_1$であるから，$u-u\zeta=u_1\in M_1$となる．よって$u=u_1+u_2$, $u_1\in M_1$, $u_2\in M_2$と書けた．次に$w\in M_1$とすると$wx\in M_1$, $wx\eta=0$となり$w\zeta=0$である．したがって任意の$u\in M$に対し$(u-u\zeta)\zeta=0$, すなわち$u\zeta^2=u\zeta$となる．したがって$u_1+u_2=0$とすると$u_1\zeta+u_2\zeta=0$となり，$0+u_2\zeta=u_2=0$, したがって$u_1=0$となる．ゆえにこの表現は完全可約である．

行列による別証：

$$\rho(x)=\left(\begin{array}{c|c}\sigma(x) & 0\\ \hline \theta(x) & \tau(x)\end{array}\right)$$

とする．ただし，$\sigma(x)$, $\tau(x)$はそれぞれr次と$n-r$次の表現である．このとき行列

$$S=\left(\begin{array}{c|c}I_r & 0\\ \hline \mu & I_{n-r}\end{array}\right)$$

で，すべての$x\in G$に対し

$$\left(\begin{array}{c|c}\sigma(x) & 0\\ \hline \theta(x) & \tau(x)\end{array}\right)\left(\begin{array}{c|c}I_r & 0\\ \hline \mu & I_{n-r}\end{array}\right)=\left(\begin{array}{c|c}I_r & 0\\ \hline \mu & I_{n-r}\end{array}\right)\left(\begin{array}{c|c}\sigma(x) & 0\\ \hline 0 & \tau(x)\end{array}\right)$$

が成り立つものをみつけたい．ただしμはxに無関係とする．このような行列Sが見つかれば，明らかにSは正則で，同値な表現

$$\rho^*(x)=S^{-1}\rho(x)S=\left(\begin{array}{c|c}\sigma(x) & 0\\ \hline 0 & \tau(x)\end{array}\right)\qquad x\in G$$

を与え，これは完全可約である．それには x に無関係な $(n-r)\times r$ 行列 μ で，すべての $x\in G$ に対し

$$\mu\sigma(x)-\tau(x)\mu=\theta(x)$$

となるものを見つけることが必要である．$\rho(yx)=\rho(y)\rho(x)$ より

$$\theta(yx)=\theta(y)\sigma(x)+\tau(y)\theta(x)$$

が成り立ち，したがって

$$\theta(x)=\tau(y^{-1})\theta(yx)-\tau(y^{-1})\theta(y)\sigma(x)$$

が任意の $y\in G$ に対し成り立つから，

$$\theta(x)=\frac{1}{g}\sum_y\left(\tau(x)\tau(x^{-1}y^{-1})\theta(yx)-\tau(y^{-1})\theta(y)\sigma(x)\right)$$

となる．そこで

$$-\mu=\frac{1}{g}\sum_y\tau(y^{-1})\theta(y)=\frac{1}{g}\sum_y\tau(x^{-1}y^{-1})\theta(yx)$$

と置くと，$\theta(x)=-\tau(x)\mu+\mu\sigma(x)$ となる．よって適当な $(n-r)\times r$ 行列 μ が見つかったわけで，変換行列 S で同値な表現 ρ^* が完全可約になるものが存在する．

この定理を繰り返し適用することにより，次の主要結果が得られる．

定理 16.3.2. 有限群 G の体 F 上の任意の表現は，体の標数が G の位数を割らないとき，完全可約であって，既約表現の和となる．

系 16.3.1. 体 F の標数が有限群 G の位数を割らないとき，G の表現が同値になるためには，それらの表現が同じ既約表現の和として表わされ，各既約表現の重複度が一致することが必要十分である．

表現 ρ が完全可約ならば，

$$\rho=\rho_1\oplus\rho_2\oplus\cdots\oplus\rho_k$$

と書けるが，ρ_i の順序は問題とならない．なぜなら，表現加群 M の基底の元

をならべかえることにより，ρ_i をならべかえることができるからである．この ρ_i というのは M を F と G が作用している加法群とみたときの組成因子であって，Jodan-Hölder の定理により，順序と作用同型を除いて一意的に定まる．定理 16.2.1 により，既約表現が作用同型であるということは，同値であるということである．そういうわけで，系において，"同じ既約表現"という言葉を使ったが，このとき同値な表現は区別していない．

16.4. 半単純な群環と通常表現

群 G と体 F が与えられたとき，次のようにして群環 R_G をつくることができる．

1) R_G は $g_i \in G$ を基底とする F 上のベクトル空間である．

2) 積は

$$\sum_i a_i g_i \sum_j b_j g_j = \sum_{i,j} a_i b_i g_{ij}$$

と置くことによって定義される．ただし，g_{ij} というのは G における積 $g_i g_j$ である．

この定義により R_G が結合環になり，F の単位元と G の単位元の積 $1\cdot 1=1$ が R_G の単位元となることを示すのはむずかしくない．G の元を右から掛けるという作用により，R_G が G の表現加群になっていることは明らかである．G が位数 n の有限群のとき，G の元 $g_1, \cdots, g_n$ を R_G の基底としてとると，対応する表現は

$$\rho(x) = (x_{ij}), \quad i, j = 1, \cdots, n, \quad x \in G$$

となる．ただし，$g_i x = g_j$ のとき $x_{ij} = 1$ で，それ以外の $x_{ij} = 0$ である．これは G の右正則表現であることが分かる．置換群としては，行列の形で書くと，

$$\pi(x) = \begin{pmatrix} g_1 & \cdots g_n \\ g_1 x & \cdots g_n x \end{pmatrix} \qquad x \in G$$

で与えられる．

補題 16.4.1. 位数 n の群 G の右正則表現 $\rho(x)$ においては，$\chi(1) = n$，$\chi(g)$

$=0,\ g\neq 1$ が成り立つ.

$\rho(x)=(x_{ij})$ とすると，$\chi(x)=\sum_i x_{ii}$ だが，$g_i x=g_j$ のとき $x_{ij}=1$ でそれ以外の $x_{ij}=0$ である．$x=1$ ならば $g_i 1=g_j=g_i$ だから，$x_{ii}=1,\ i=1,\cdots,n$ となり，$\chi(1)=n$ である．しかし $x=g\neq 1$ ならばどの g_i に対しても $g_i x=g_i$ とはならないから $x_{ii}=0$ である.

以後得られる結果はほとんどすべて有限群 G の体 F 上の表現で，体の標数が G の位数を割らないものに関する結果である．このような表現は**通常表現** (ordinary representation) とよばれる．標数が有限群 G の位数を割るような体 F 上の G の表現は**モジュラ表現** (modular representation) とよばれる．モジュラ表現の性質は通常表現とは異なっており，また無限群の表現が有限群の場合とはいろいろな点で異なっているのも当然であろう.

環 R は，任意の $u\in R$ に対して $uxu=u$ となる $x\in R$ が存在するとき，**正則** (regular) であるということにする．体 F 上の有限次元の正則環は**半単純** (semi-simple) であるといわれる．また $e^2=e$ を満たす元 $e\neq 0$ は**巾等元** (idempotent) とよばれる.

定理 16.4.1. 有限群 G の体 F 上の群環 R_G が半単純になるためには，F の標数が G の位数を割らないことが必要十分である.

証：G を位数 g の有限群とする．F の標数が g を割るときには，G の元を $x_1,\cdots,x_g$ とし，R_G の元 $u=x_1+\cdots+x_g$ を考えることにする．$x_i u=ux_i=u$ であるから，$x=a_1x_1+\cdots+a_gx_g$ とすると，$ux=(a_1+\cdots+a_g)u$ となり，$uxu=(a_1+\cdots+a_g)gu=0\neq u$ である．ゆえに R_G は半単純ではない.

そこで G の位数 g が F の標数で割れないとしよう．このとき R_G が半単純であることを証明するわけだが，実際，R_G のもっと詳しい性質が証明される．$\mathfrak{a}_1$ を R_G の任意の右イデアルとする．$\mathfrak{a}_1$ は R_G の表現部分加群となるが，逆に R_G の表現部分加群というのは右イデアルである．完全可約性の定理により，別のイデアル $\mathfrak{a}_2$ が存在して，

$$R_G=\mathfrak{a}_1\oplus\mathfrak{a}_2$$

と書ける．したがって $1=a_1+a_2$, $a_1\in\mathfrak{a}_1$, $a_2\in\mathfrak{a}_2$ と一意的に表わされる．すると $a_1=a_1{}^2+a_2a_1$ となるが，$a_1=a_1+0$ と一意的に表わされるはずだから，これと比べてみると，$a_1{}^2=a_1$, $a_2a_1=0$ となることがわかる．したがって $a_1=e$ は巾等元，$a_2=1-e$ も巾等元である．そして $x\in R_G$ に対し，$ex\in\mathfrak{a}_1$ で $x=ex+(1-e)x$ とかける．逆に，$y\in\mathfrak{a}_1$ ならば，$y=ey+(1-e)y=y+0$ となるから，表現の一意性より，$y=ey$ となる．したがって $\mathfrak{a}_1$ は巾等元 e が生成する主右イデアル[1] eR_G であって，R_G の任意の右イデアルはある巾等元の生成する主右イデアルである．特に任意の元 u に対し $uR_G=eR_G$ となる巾等元 e が存在する．ゆえに $ux=e$ となる x および $ey=u$ となる y が存在し，$eu=e^2y=ey=u$ となる．したがって $u=eu=uxu$ となり，R_G は正則である．

定理 16.4.2. 体 F 上有限次元の正則環 R は単位元を持ち，任意の右（左）イデアルはある巾等元の主イデアルとなる．任意の両側イデアルは中心にはいる巾等元の主イデアルとなる．

証：R を体 F 上有限次元の正則環とする．任意の元 u に対し，正則性から $uxu=u$ となる x が存在する．そこで $e=ux$ と置くと，$e^2=uxux=ux=e$ となり，$f=xu$ と置くと $f^2=xuxu=xu=f$ となる．さらに $u=uxu=eu=uf$ だから，$eR=uR$, $Ru=Rf$ が成り立つ．したがって主右（左）イデアルは巾等元の主右（左）イデアルとなることがわかった．そこで左イデアル $\mathfrak{a}$ を考えよう．$\mathfrak{a}\neq 0$ ならば $\mathfrak{a}$ は巾等元 $e_1\neq 0$ を含み，$Re_1\subseteq\mathfrak{a}$ となる．$\mathfrak{a}\neq Re_1$ としよう．すると $x\notin Re_1$ なる $x\in\mathfrak{a}$ が存在する．

$$x=xe_1+(x-xe_1)$$

と書くと，$x_1=xe_1\in Re_1$ で，

$$x_2=x-xe_1$$

と置くと，$x_2e_1=0$ である．

f を $Rx_2=Rf$ となる巾等元としよう．すると $f=wx_2$ と書けるから，

---

1) 主イデアルというのは1つの元から生成されるイデアルのことである．

$fe_1=wx_2e_1=0$ となる．そこで $e_2=e_1+f-e_1f$ と置くと，$e_1e_2=e_1$，$fe_2=f$ となる．したがって

$$e_2{}^2=(e_1+f-e_1f)e_2=e_1+f-e_1f=e_2$$

となり，e_2 は $\mathfrak{a}$ にはいる巾等元であって，Re_2 は e_1 も f も含み，したがって Re_1 および $x\notin Re_1$ を含む．ゆえに Re_2 の次元は R_1 より大きい．これを続けていけば，$\mathfrak{a}$ の巾等元 $e_3, e_4, \cdots$ で各イデアル Re_i は直前のものより大きい次元を持つようにできて，最後には $\mathfrak{a}=Re$ となる巾等元 e にたどり着く．これで任意の左イデアルが巾等元の主左イデアルとなることが証明された．同様にして，任意の右イデアルが巾等元の主右イデアルとなることも示される．$x\in eR$ ならば適当な w により $x=ew$ と書けるから，$ex=e^2w=ew=x$ となり，e は eR の元に対する左単位元である．同様にして $x\in Rf$ ならば $xf=x$ となる．R 自身を左イデアルまたは右イデアルと考えると，巾等元 e, f で $R=eR=Rf$ となるものが存在する．よって $ef=f=e$ となり，$ex=xe=x$ だから，$e=1$ は R の単位元である．

R の中心にはいる巾等元 e の倍元全体は確かに両側イデアルをつくる．逆に任意の両側イデアル $\mathfrak{a}$ は中心にはいる巾等元の主イデアルであることを示そう．適当な巾等元 e, f により $\mathfrak{a}=eR=Rf$ と書けるが，$ef=f=e$ となるから，$\mathfrak{a}=eR=Re$ である．R の任意の元 x に対し $ex\in\mathfrak{a}$ だから，$ex=exe$ となる．また $xe\in\mathfrak{a}$ より $xe=exe$ となる．ゆえに $ex=xe$ となり，e は R の中心にはいる．

環 R が半単純で，0 と R 以外に両側イデアルを含まないとき，**単純** (simple) であるという．右イデアルの直和は $\oplus$ で，両側イデアルの直和は $\boxplus$ で表わすことにする．

定理 16.4.3. 半単純環 R は単純環の直和として $R=R_1\boxplus R_2\boxplus\cdots\boxplus R_s$ と表わされる．そしてこの単純環 R_i は順序を除けば一意的に定まる．

証：R_1 を R に含まれる極小両側イデアルとすると R_1 は R の中心にはいる巾等元 e_1 の主イデアルとなる．$x\in R$ は $x=xe_1+x(1-e_1)$ と書けるから，

$x(1-e_1)$ という形の元の全体を R_1 と置くと，$R=R_1 \boxplus \bar{R}_1$ となる．e_1 は R_1 の単位元，$\bar{e}_1=1-e_1$ は $\bar{R}_1$ の単位元で，$x, y \in R_1$, z, $w \in \bar{R}_1$ に対し，$(x+z)+(y+w)=(x+y)+(z+w)$, $(x+z)(y+w)=xy+zw$ が成り立つ．なぜなら $zy=ze_1(1-e_1)y=0$, 同様に $xw=0$ が成り立っているからである．したがって直和 $R_1 \boxplus \bar{R}_1$ において，和や積は成分ごとに別々にやればよい．したがって特に R の正則性から R_1 および $\bar{R}_1$ の正則性が得られる．次に R_2 を $\bar{R}_1$ の極小両側イデアルとすると，$\bar{R}_1=R_2 \boxplus \bar{R}_2$ となる．これを続けていくと，最後には

$$R=R_1 \boxplus R_2 \boxplus \cdots \boxplus R_s$$

となり，$1=e_1+e_2+\cdots+e_s$ と書ける．ただし $e_i, i=1, \cdots, s$ は R の中心にはいる巾等元で，$i \neq j$ なら $e_ie_j=0$ である．

$$x=x_1+x_2+\cdots+x_s,$$
$$y=y_1+y_2+\cdots+y_s$$

に対して

$$x+y=(x_1+y_1)+(x_2+y_2)+\cdots+(x_s+y_s),$$
$$xy=x_1y_1+x_2y_2+\cdots+x_sy_s$$

が成り立つ．ただし $x_i, y_i \in R_i$ とする．逆に，同じ体 F 上の単純環 R の直和は正則で，したがって半単純となる．$\mathfrak{a}$ を R の任意の両側イデアルとすると，$\mathfrak{a}$ は中心にはいる巾等元 e の主イデアルとなる．そして

$$e=e_1e+e_2e+\cdots+e_se$$

で，ある i に対し $e_ie \neq 0$ となる．そこでもし $\mathfrak{a}$ が極小だとすると，$e_ie \neq e_i$ ならば e_ie の主イデアルは R_i に真に含まれることになるから，$e_ie=e_i$ で，また $e_ie \neq e$ とすると，e_ieR が $\mathfrak{a}$ に真に含まれることになるから，$e_i=e$ でなければならない．ゆえに $e_ie=e_i=e$ となり，$\mathfrak{a}=R_i$ となる．これで直和の一意性が証明された．

定理 16.4.4. 有限群 G の任意の通常既約表現は R_G のある極小右イデアルによる表現に同値である．R_G の2つの極小右イデアルが同値な表現を与える

ためには，それらが R_G の同じ単純成分にはいることが必要十分である．

証：G の任意の表現 ρ から R_G の表現がつくられることを注意しておく．なぜなら R_G の任意の元

$$h=\sum_{x\in G}a_x x,\quad a_x\in F,\quad x\in G$$

に対し，$\rho(h)=\sum a_x\rho(x)$ と置けば，これは R_G の表現となる．G の同値な表現は R_G の同値な表現を与え，逆も成り立つ．

Gの正則表現というのは R_G を $F-G$ 加群とみたときの表現である．R_G を完全に約すと，

$$R_G=e_1R_G\oplus e_2R_G\oplus\cdots\oplus e_tR_G$$

となったとする．ただし $1=e_1+e_2+\cdots+e_t$ で e_i は互いに**直交**する（orthogonal）巾等元である．すなわち $i\neq j$ ならば $e_ie_j=0$ となる．そして各 e_iR_G は極小右イデアルである．そこで $\rho(x)$ を G，したがって R_G の通常既約表現とする．ρ を与える既約 $F-G$ 加群をMとする．すると $M=M\cdot 1=M(e_1+\cdots+e_t)$ となる．したがってある e_i に対し $Me_i\neq 0$ である．m を $me_i\neq 0$ となるMのあるベクトルとする．すると $me_iR_G\neq 0$ となるが，M は既約だから，$M=me_iR_G$ でなければならない．

$$me_i(\sum_{x\in G}a_x x)\leftrightarrows e_i\sum_{x\in G}a_x x$$

という対応は一対一である．なぜなら $me_ih=0$ となる e_ih の全体は e_iR_G に真に含まれる右イデアルだから0となるからである．この対応により，表現加群M と表現加群 e_iR_G の間の作用同型が得られたわけで，定理16.1.1により，$\rho(x)$ は極小右イデアル e_iR_G によるGの表現と同値になる．

2つの極小右イデアルが同値な表現を与えるのはいつだろうか？　極小右イデアルはただ1つの極小両側イデアルに含まれる．R_G が単純イデアル，すなわち極小両側イデアルの和として

$$R_G=R_1\boxplus R_2\boxplus\cdots\boxplus R_s$$

と分解されたとする．このとき $1=e_1+e_2+\cdots+e_s$ と表わされる．ただし e_i は中心にはいる互いに直交する巾等元の集合である．$e_{i_1}R_G$ と $e_{i_2}R_G$ を同じ

単純イデアル R_i にはいる2つの極小右イデアルとする．すべての有限和 $u_1e_{i1}v_1+\cdots+u_me_{i1}v_m$, u_k, $v_k\in R_G$ は両側イデアルをつくり，$e_i(e_{i1})e_i=e_{i1}\neq 0$ はこの中にはいるから，この集合は R_i になる．したがって適当な u 達と v 達をとれば

$$u_1e_{i1}v_1+\cdots+u_me_{i1}v_m=e_{i2}$$

となり，$e_{i2}^2=e_{i2}$ だから，ある j に対し

$$e_{i2}u_je_{i1}v_j\neq 0$$

となる．ところがそうすると $e_{i1}v_jR_G\neq 0$ で，これは極小イデアル $e_{i1}R_G$ に含まれる右イデアルだから，$e_{i1}v_jR_G=e_{i1}R_G$ となる．同様にして $e_{i2}u_je_{i1}v_jR_G=e_{i2}R_G$ を得る．したがって $w=e_{i2}u_j$ と置くと，$we_{i1}R_G=e_{i2}R_G$ となり，$h\in R_G$ に対し，$we_{i1}h\leftrightarrows e_{i2}h$ は右イデアル $e_{i1}R_G$ と $e_{i2}R_G$ の間の作用同型となり，これらが与える表現は同値である．これにより，同じ単純イデアルに含まれる2つの極小イデアルは同じ表現を与えることが分かった．

次に $e_{i1}R_G$ と $e_{j1}R_G$ を，それぞれ単純イデアル R_i と R_j, $i\neq j$ に含まれる極小右イデアルとする．$e_{i1}R_G$ による表現 ρ において，e_i, e_j に対応する写像は，それぞれ

$$e_i: e_{i1}h\to e_{i1}he_i=e_{i1}e_ih=e_{i1}h$$

$$e_j: e_{i1}h\to e_{i1}he_j=e_{i1}e_jh=0$$

となり，$\rho(e_i)=1$, $\rho(e_j)=0$ である．同様に $e_{j1}R_G$ により，e_i は0で，e_j は1で表現される．ゆえにこれらの表現は同値ではない．

R_G の単純イデアルの直和への分解を R_G の中心 Z にはいる直交巾等元を見つけることに関係づけたが，R_G の中心とはどのようなものだろうか？　これには容易に答えることができる．

定理 16.4.5. $x_{i1}, x_{i2}, \cdots, x_{ih}$ を群 G の共役な元の類とするとき，$C_i=x_{i1}+\cdots+x_{ih}$ という元が R_G の中心の基底となる．

証：$x_{i1}, x_{i2}, \cdots, x_{ih}$ を G の共役元の類とし，$C_i=x_{i1}+\cdots+x_{ih}$ とすると，G の元による変換により，ある類の元はその中で互いに移りあうだけだから，

$y \in G$ に対し，$y^{-1}C_i y = C_i$ となる．C_i が任意の $y \in G$ と可換になるから，C_i は R_G の任意の元と可換になり，R_G の中心にはいる．逆に $u = \sum_{x \in G} a_x x$ が R_G の中心にはいり，$y \in G$ とすると，$y^{-1}uy = u = \sum_{x \in G} a_x y^{-1}xy$ となり，u において共役な元の係数は等しく，u は C_i の線形結合となる．

16.5. 絶対既約表現．単純環の構造

群 G の通常既約表現はすべて正則表現 $R(G)$ の成分として現われるということはわかった．したがって G の通常既約表現を決定するには，$R(G)$ を完全に約すこと，または，結局同じことになるが，群環 R_G の既約右イデアルを見つけることが問題になる．

表現の既約性というのは体と関係した相対的なものである．たとえば，G を元 $1, x, x^2$ から成る位数 3 の巡回群とし，有理数体上で考えると，R_G は $R_G = R_1 \boxplus R_2$ と分解され，

$$e_1 = \frac{1+x+x^2}{3}, \quad e_2 = \frac{2-x-x^2}{3}$$

は巾等元で，$1 = e_1 + e_2$ となり，R_1 は e_1 を基底に，R_2 は e_2, e_2x を基底にもつ．これにより表現

$$\rho(x) = \left(\begin{array}{c|cc} 1 & 0, & 0 \\ \hline 0 & 0, & 1 \\ 0 & -1, & -1 \end{array}\right)$$

が与えられ，R_1, R_2 は次数が 1 および 2 の既約表現を与える．しかし有理数体に 1 の 3 乗根 $\varepsilon = (-1+\sqrt{-3})/2$ をつけ加えて拡大すると，R_2 上の既約表現は可約となる．R_G の基底として

$$e_1 = \frac{1+x+x^2}{3}$$

$$\bar{e}_2 = \frac{1+\varepsilon x+\varepsilon^2 x^2}{3}, \quad \bar{e}_3 = \frac{1+\varepsilon^2 x+\varepsilon x^2}{3}$$

がとれ，$\bar{e}_2 + \bar{e}_3 = e_2$ となる．この新しい基底に関しては

$$\rho(x)=\begin{pmatrix}1, & 0, & 0\\ 0, & \varepsilon^2, & 0\\ 0, & 0, & \varepsilon\end{pmatrix}\qquad \varepsilon^3=1$$

となる．明らかに，さらに体を拡大しても $\rho(x)$ がこれ以上約されることはない．

n 次の表現 ρ は，体 F を拡大しても可約となることがないならば，**絶対既約** (absolutely irreducible) であるという．ρ が $K\supset F$ 上で可約となり，すべての $x\in G$ に対し

$$\rho(x)=\left(\begin{array}{c|c}\sigma(x) & 0\\ \hline 0 & \tau(x)\end{array}\right)$$

となったとする．ただし，$\sigma(x)$ は $s\times s$ 行列，$\tau(x)$ は $(n-s)\times(n-s)$ 行列である．すると，$\rho(h)$, $h\in R_G$ は K 上の多元環としてたかだか $s^2+(n-s)^2<n^2$ 次元である．ゆえにもし $\rho(h)$, $h\in R_G$ が F 上の多元環として n^2 次元ならば，ρ は F 上絶対既約である．任意の通常表現は体を適当に代数拡大すれば，既約表現の直和になって，それらの既約表現のうち，n 次のものはその体上 n^2 次元となるようにできることを示そう．

定理 16.5.1. 体 F 上有限次元の斜体 D が F の任意の代数拡大体上の斜体となるのは，D が F 上一次元で $D=F$ のときだけである．

証：D の F 上の基底を $u_1, \cdots, u_n$ とする．ただし $u_1=1$ は D の単位元とする．$n>1$ ならば $1=u_1, u_2, u_2^2, \cdots, u_2^n$ は線型従属でなければならないから

$$u_2^r+a_1u_2^{r-1}+\cdots+a_r=0,\quad a_i\in F$$

という関係がある．そこで F に $f(x)=x^r+a_1x^{r-1}+\cdots+a_r$ の根 $\alpha_1, \cdots, \alpha_r$ をつけ加えると，$(u_2-\alpha_1u_1)\cdots(u_2-\alpha_ru_1)=0$ となる．ゆえに F のこの代数拡大体上 $u_2-\alpha_iu_1$ は零因子となり，D が F の任意の代数拡大体上斜体であるためには $n=1$ でなければならない．したがって $D=F$ となる．

定理 16.5.2. 単純環 R は R に含まれる適当な斜体 D 上の全行列環となる．

証：$e_{11}R$ を R の極小右イデアルとする．ただし e_{11} は巾等元とする．すると $1-e_{11}$ も巾等元で，$R=e_{11}R\oplus(1-e_{11})R$ となる．e_2R を $(1-e_{11})R$ の極小右イデアル，e_2 は巾等元とすると，$(1-e_{11})e_2=e_2$ だから，$e_{11}e_2=0$ となる．したがって $e_{22}=e_2=e_2e_{11}$ は巾等元で，$e_{22}R=e_2R$, $e_{11}e_{22}=0$, $e_{22}e_{11}=0$ となる．そして $R=e_{11}R\oplus e_{22}R\oplus(1-e_{11}-e_{22})R$ が成り立つ．そこで直交する巾等元 $e_{11},\cdots,e_{ii}$ で，$e_{ii}R$ は極小，かつ $R=e_{11}R\oplus e_{22}R\oplus\cdots\oplus e_{ii}R\oplus(1-e_{11}-\cdots-e_{ii})R$ となるものが見つかったとしよう．$e_{i+1}R$ を $(1-e_{11}-\cdots-e_{ii}R)$ の中の極小右イデアル，e_{i+1} は巾等元とする．すると，$e_{i+1}=(1-e_{11}-\cdots-e_{ii})e_{i+1}$ だから，$e_{jj}e_{i+1}=e_{jj}(1-e_{11}-\cdots-e_{ii})e_{i+1}=0$, $j=1,\cdots,i$ が成り立つ．そこで $e_{i+1,i+1}=e_{i+1}(1-e_{11}-\cdots-e_{ii})$ と置くと，$e_{i+1,i+1}$ は巾等元で $e_{i+1,i+1}R=e_{i+1}R$ となり，また $e_{i+1,i+1}$ は $e_{11},\cdots,e_{ii}$ と直交する．したがってこれを続けていけば，

$$R=e_{11}R\oplus e_{22}R\oplus\cdots\oplus e_{nn}R$$

となる．ただし e_{ii} は直交する巾等元，$e_{ii}R$ は極小右イデアルで $1=e_{11}+e_{22}+\cdots+e_{nn}$ である．

補題 16.5.1. $i,j=1,\cdots,n$ について $e_{ii}Re_{jj}\neq0$ が成り立つ．

証：有限和 $\sum_k u_ke_{ii}v_k$ の全体は $e_{ii}\neq0$ を含む両側イデアルをつくるから，環 R 全体になる．したがって適当に u_k, v_k をとると $\sum u_ke_{ii}v_k=e_{jj}$ となり，$\sum u_ke_{ii}v_ke_{jj}=e_{jj}$ となる．ゆえに $e_{ii}ve_{jj}\neq0$ となる v が存在する．

補題 16.5.2. $e_{ii}Re_{ii}$ は斜体 D_i である．

証：$e_{ii}Re_{ii}$ は加法と乗法に関しては確かに閉じているから，R_1 の部分環であって，e_{ii} を単位元として持っている．したがって 0 以外の元が逆元を持つことをいえばよい．$e_{ii}xe_{ii}\neq0$ とすると，$e_{ii}xe_{ii}R\neq0$ は極小右イデアル $e_{ii}R$ に含まれる右イデアルだから，$e_{ii}R$ に一致する．ゆえに $e_{ii}xe_{ii}y=e_{ii}$ となる y が存在し，$e_{ii}xe_{ii}\cdot e_{ii}ye_{ii}=e_{ii}$ が成り立つ．ゆえに $e_{ii}ye_{ii}$ は $e_{ii}xe_{ii}$ の $e_{ii}Re_{ii}$ における逆元で，$e_{ii}Re_{ii}$ は斜体 D_i となる．

各 $i=2, \cdots, n$ に対し，$e_{11}be_{ii}\neq 0$ なる元を選び，$e_{11}be_{ii}=e_{1i}$ と書くことにすると，

$$e_{11}e_{1i}=e_{1i}e_{ii}=e_{1i}$$

が成り立つ．$e_{1i}R\subseteq e_{11}R$ だから $e_{1i}R=e_{11}R$ が成り立ち，$e_{1i}y=e_{11}$ となる y が存在する．$e_{1i}(e_{ii}ye_{11})=e_{11}$ となるから，$e_{i1}=e_{ii}ye_{11}$ と書くことにすると，$i=2, \cdots, n$ について

$$e_{ii}e_{i1}=e_{i1}e_{11}=e_{i1}, \quad e_{1i}e_{i1}=e_{11}$$

が成り立つ．したがって $e_{1i}e_{i1}e_{1i}e_{i1}=e_{11}{}^2=e_{11}$ となり，$e_{i1}e_{1i}\neq 0$ である．しかし $(e_{i1}e_{1i})^2=e_{i1}e_{1i}$ は $e_{ii}Re_{ii}$ にはいる巾等元で，斜体における 0 でない巾等元は単位元だけであるから，$e_{i1}e_{1i}=e_{ii}$ となる．そこで $i\neq j$ ならば $e_{i1}e_{1j}=e_{ij}$ と置く．すると，$e_{ij}e_{jk}=e_{i1}e_{1j}e_{j1}e_{1k}=e_{i1}e_{11}e_{1k}=e_{i1}e_{1k}=e_{ik}$ となる．また $j\neq k$ ならば $e_{ij}e_{kt}=e_{ij}e_{jj}e_{kk}e_{kt}=0$ となる．したがってこれら n^2 個の元 e_{ij} に対し，常に

$$e_{ij}e_{kt}=\delta_{jk}e_{it} \qquad \delta_{jj}=1, \ \ \delta_{jk}=0, \ \ j\neq k$$

が成り立つことがわかった．したがって e_{ij} は n^2 個の $n\times n$ 行列

$$E_{ij}=(a_{rs}), \ \ a_{ij}=1, \ \ (r, s)\neq(i, j) \text{ ならば } a_{rs}=0$$

の乗法と同じ性質を持っている．

次に斜体 $D_1=e_{11}Re_{11}$ から環 D を，各 $d_1\in D_1$ に対し

$$d=d_1+e_{21}d_1e_{12}+\cdots+e_{n1}d_1e_{1n}$$

と置くことにより定義する．D が D_1 と同型になることは容易に確められ，D も斜体となる．D_1 の単位元 e_{11} に対応する $e_{11}+e_{22}+\cdots+e_{nn}=1$ は D の単位元でもあり，R の単位元でもある．また $d\in D$ に対し $e_{ij}d=e_{i1}d_1e_{1j}=de_{ij}$ が成り立つことがわかる．

最後に，任意の $x\in R$ に対し，$x=1x1=(e_{11}+\cdots+e_{nn})x(e_{11}+\cdots+e_{nn})=\sum_{i,j} e_{ii}xe_{jj}$ となる．そして

$$x_{ij}=e_{ii}xe_{jj}=e_{i1}e_{1i}xe_{j1}e_{1j}=e_{i1}u_1e_{1j}$$

となる．ただし $u_1\in D_1$ である．したがって $u\in D$ に対しては $x_{ij}=ue_{ij}=e_{ij}u$ となる．これで定理が完全に証明された．単純環 R は斜体 D 上の $n\times n$ 行列

環の形に具体的に表わされ，Dの単位元はRの単位元に一致する．

定理 16.5.3. R_G を体F上の半単純な群環とすると，R_G が F^* 上の全行列環の直和となるようなFの代数拡大体 F^* が存在する．F^* としてはFの有限次代数拡大体がとれる．

証：R_G が体F上半単純になるためには，体の標数が群Gの位数を割らないことが必要十分だった．この性質はFをその代数拡大体 F^* で置き換えても変わらない．R_G を体F上で単純環の直和として R_1 田 … 田 R_s と分解したとき，対応する斜体がFにならないような単純成分 R_k があったとすると，Fをある F^* に代数拡大したとき，Dは斜体であるという性質を失う．これによる R_G の分解の変わり方は次の2つのいずれかである．（1）Rの中心にはいる巾等元の数が増え（減ることはない），単純環だったものが，いくつかの単純環の直和にわかれる．（2）単純環Rにおいてもっと次元の小さい斜体 D^* が見つかり，Rが D^* 上のもっと大きい行列環として表わされる．この両方の場合とも起こり得る．位数3の群の表現において，最初の場合が起こることはすでに見た．2番目の場合は四元数群Qの有理数体F上の群環 R_Q において起こる．R_Q はF上で1次元の単純環4つと，それ自身斜体（四元数環と呼ばれる）である4次元のもの1つの直和になる．Fにiをつけ加えると，この斜体は複素有理数体上 2×2 行列の環になる．

いずれにせよ，Fの代数的閉包$\bar{F}$上では，R_G に現われる単純環 R_k はすべて$\bar{F}$上の行列環になる．単純環 R_k の行列単位 $e_{ij}{}^k$ はGの元xを使って表わすことができ，この表現に現われるすべての係数を含む任意の体 F^* 上で R_k は全行列環となり，F^* は明らかにFの有限次拡大である．

定理 16.5.4. 体F上の全行列環 R_k の中心は R_k の単位元（つまり単位行列）のスカラー倍の全体から成る．体F上の行列環の直和 $R=R_1+\cdots+R_r$ の中心は，$R_1, \cdots, R_r$ の単位元r個を基底にもつ．

証：R_k をF上の $n\times n$ 全行列環とする．そして

$$x=\sum_{i,j}a_{ij}e_{ij},\quad a_{ij}\in F$$

を R_k の中心の元とする. $e_{rs}x=xe_{rs}$ より

$$\sum_j a_{sj}e_{rj}=\sum_i a_{ir}e_{is}$$

となることがわかる. したがって $j\neq s$ ならば $a_{sj}=0$ で $a_{ss}=a_{rr}$ である. よって $x=a_{11}(e_{11}+\cdots+e_{nn})=a_{11}\cdot 1$ となるが, 逆にこのような元はすべて R_k の中心にはいる. 次に

$$R=R_1+\cdots+R_r$$

とすると, R の中心は R_k の中心の直和で, R_k の単位元 r 個を基底にもつ.

G の通常表現を半単純な群環 R_G に関係づけるいくつかの定理が得られた. これらの結果を1つの定理としてまとめておく.

定理 16.5.5. 有限群 G の通常既約表現はすべて右正則表現 $R(G)$ の成分として現われる. 同値でない絶対既約表現の数は G の共役類の数に等しい. $\rho_1,\cdots,\rho_r$ を相異なる絶対既約表現とし, ρ_i の次数を $n_i, i=1,\cdots,r$ とすると, ρ_i は F 上 n_i^2 次元で, ρ_i は $R(G)$ の中に n_i 個現われる. すべての $\rho_i(x)$, $x\in G$ と可換な行列は単位行列のスカラー倍だけである. G の位数を g とすると, $g=n_1^2+n_2^2+\cdots+n_r^2$ が成り立つ.

証: 定理 16.4.4 により, 通常既約表現はすべて R_G の適当な極小右イデアル上の表現に同値となり, $R(G)$ の成分として現われる. また R_G における単純イデアルの数だけ同値でない既約表現が存在する. 必要ならば体 F を F^* まで拡大することにより, R_G が r 個の行列環の直和となるとき, 定理 16.5.4 により, R_G の中心は r 個の巾等元から成る基底をもつ. 一方定理 16.4.5 により, R_G の中心は共役類の元の和 C_i を基底にもち, r は G における共役類の数となる. F^* 上で R_i の中に現われる極小右イデアルの1つは $e_{11}R$ で, もし R_i が $n_i\times n_i$ 行列環とすると, $e_{11}R$ は $e_{11}, e_{12},\cdots, e_{1n_i}$ を基底にもつ. 対応する表現 ρ_i は n_i 次で, R_G の表現にまで拡張された ρ_i は単純環 R_i を忠実に表現し, 定理 16.4.4 の証明において示されたように e_j を R_j の単位元とすると

き，$j \neq i$ ならば，$\rho_i(e_j)=0$ となるから，他の R_j はすべて0に表現される．したがって，$\rho_i(R_G)$ は F^* 上 n_i^2 次元の全行列環となり，これがさらに約されるのは F^* 上の次元がもっと小さいときだけだから，これは確かに絶対既約である．また n_i^2 次元であるから，すべての $\rho_i(x)$, $x \in G$ と可換になる行列は単位行列のスカラー倍だけである．最後に，各 R_i は n_i^2 個の元から成る基底をもっているから，その直和は $n_1^2+\cdots+n_r^2$ 個の元から成る基底をもつ．一方 R_G は G の g 個の元を基底としてもつ．ゆえに

$$g=n_1^2+\cdots+n_r^2$$

が成り立つ．R_i は n_i 個の右イデアル $e_{11}R, \cdots, e_{n_in_i}R$ の直和であるから，ρ_i は $R(G)$ に n_i 回現われる．

16.6. 通常指標の関係式

前節では，R_G の性質と，G の表現が R_G の表現を与えるということから G の表現に関する情報が与えられた．この節では，指標 $\chi(x)$, $x \in G$ の満たす関係式を見つけることにする．これらは R_G よりも G 自身に密接に関係している．この節においては通常表現だけを扱う．

定理 16.6.1. A, B を2つの F-G 加群とする．A は m 次元で，表現 $\rho(x)$, $x \in G$ を与え，B は n 次元で，表現 $\sigma(x)$ を与えるとすると，A から B への作用準同型全体のつくる加法群は，すべての $x \in G$ に対し，$\rho(x)\alpha=\alpha\sigma(x)$ を満たす $m \times n$ 行列の全体のつくる加法群と同型である．

系 16.6.1. A から A 自身への作用自己準同型全体のつくる環は $\rho(x)\alpha=\alpha\rho(x)$ を満たす $m \times m$ 行列 α 全体のつくる環と同型である．

証：A の基底を $u_1, \cdots, u_m$, B の基底を $v_1, \cdots, v_n$ とする．A から B への任意の線形写像は基底の像で決定される．そこで，

$$u_1 \to a_{11}v_1+\cdots+a_{1n}v_n$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$u_i \to a_{i1}v_1 + \cdots + a_{in}v_n$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$u_m \to a_{m1}v_1 + \cdots + a_{mn}v_n$$

とし，$\alpha=(a_{ij})$, $i=1, \cdots, m$; $j=1, \cdots, n$ と書くことにする．これらの線形写像の全体は行列 α の全体のつくる加法群と同型な加法群をつくる．線形写像であるだけでなく，作用準同型であるためには，$u \to v$ のとき，任意の $x \in G$ に対し $ux \to vx$ となることが必要である．これは，写像 $u \to ux \overset{\alpha}{\to} vx$ と $u \overset{\alpha}{\to} v \to vx$ が一致するということを意味するが，これはすべての $x \in G$ について，

$$\rho(x)\alpha = \alpha\sigma(x)$$

という関係が成り立つということである．

A を A 自身に写すとき，写像は**自己準同型**（endomorphism）とよばれる．α, β を２つの作用自己準同型とすると，

$$\rho(x)(\alpha\beta) = [\rho(x)\alpha]\beta = [\alpha\rho(x)]\beta = (\alpha\beta)\rho(x)$$

となり，$\rho(x)\alpha = \alpha\rho(x)$ を満たす行列 α の全体は A の作用自己準同型の全体のつくる環と同型になる．

Ω を作用素の任意の集合とするとき，定理 16.6.2 は任意の Ω 加群に対して成り立つが，我々が主として関心のあるのは，もちろん F-G 加群の場合である．

定理 16.6.2.（Schur の補題） A, B を２つの既約 Ω 加群とするとき，これらが作用同型でなければ，A から B への作用準同型は A を０に写すものだけである．A が既約ならば，恒等的に０ではない A の作用自己準同型はすべて作用同型である．

証：$u \in A$, $v \in B$, $\omega \in \Omega$ とする．ある $u \in A$ に対し，ある作用準同型が $u \to v \neq 0$ に写したとすると，すべての $\omega \in \Omega$ に対し，$u\omega \to v\omega$ となる．$u\Omega$ は A の部分加群で A は既約だから，$u\Omega$ は A 全体になる．したがって $A = u\Omega \to v\Omega \neq 0$ となり，$A \to v\Omega = B$ となる．A の０でない元が０に写されたとす

ると，このような元の全体がAのΩ部分加群をつくり，Aが既約だとした仮定に反するから，この写像は一対一である．ゆえにこの写像は同型写像で，特にAからそれ自身への作用準同型はすべて作用同型になる．

定理 16.6.3. ρ と σ を有限群 G の同値でない既約表現で，次数をそれぞれ m, n とし，ξ を任意の $m\times n$ 行列とすると，

$$\sum_{y\in G}\rho(y)\xi\sigma(y^{-1})=0$$

が成り立つ．

証：

$$\alpha=\sum_{y\in G}\rho(y)\xi\sigma(y^{-1})$$

と書く．すると $x\in G$ に対し，$xy=z$ と置くと，$y^{-1}=z^{-1}x$ で

$$\begin{aligned}\rho(x)\alpha&=\sum_{y}\rho(x)\rho(y)\xi\sigma(y^{-1})\\&=\sum_{y}\rho(xy)\xi\sigma(y^{-1})\\&=\sum_{z}\rho(z)\xi\sigma(z^{-1})\sigma(x)\\&=\alpha\sigma(x)\end{aligned}$$

が，すべての $x\in G$ に対し成り立つ．

したがって，ρ と σ が同値でない既約表現ならば，定理 16.6.1 と 16.6.2 により，$\alpha=0$ でなければならない．これらの定理は任意の体上の G の表現に対して成り立つことを注意しておく．

$f_1(y)$ と $f_2(y)$ を $y\in G$ に対し定義され，F に値をとる 2 つの関数とするとき，**対称双線形スカラー積** (symmetric bilinear scalar product) を

$$(f_1, f_2)=\frac{1}{g}\sum_{y\in G}f_1(y)f_2(y^{-1})$$

で定義する（ただし，ここでは F の標数が G の位数を割らないと仮定している）．y がG全体を動くとき y^{-1} もG全体を動くことに注意すると，

1) $(f_1, f_2)=(f_2, f_1)$.

2) $(f_1+f_2, f_3)=(f_1, f_3)+(f_2, f_3)$.

3) $(af_1, f_2)=a(f_1, f_2)$；$a\in F$.

の成り立つことが確かめられる．そこで $\rho(x)$ と $\sigma(x)$ を同値でない既約表現としよう．定理 16.6.3 において，ξ として (r, s) 要素が 1，他の要素は 0 という $m\times n$ 行列 e_{rs} をとると，$\alpha=(\alpha_{ij})$ となることがわかる．ただし，$\alpha_{ij}=\sum_{j\in G}\rho_{ir}(y)\sigma_{sj}(y^{-1})$ で，

$$\rho(x)=(\rho_{ij}(x)) \qquad i, j=1, \cdots, m,$$
$$\sigma(x)=(\sigma_{ij}(x)) \qquad i, j=1, \cdots, n$$

とする．定理 16.6.1 と 16.6.2 により $\alpha=0$ だから，$(\rho_{ir}, \sigma_{sj})=0$ となるが，実はもっと強いことがいえる．

定理 16.6.4. ρ と σ を有限群 G の同値でない通常既約表現とすると，すべての i, r, s, j に対し，対称双線形スカラー積 $(\rho_{ir}, \sigma_{sj})=0$ となる．また ρ を n 次の絶対既約通常表現とすると，$i=j$，$r=s$ でなければ $(\rho_{ir}, \rho_{sj})=0$ で，すべての i, j に対し $(\rho_{ij}, \rho_{ji})=1/n$ となる．

証：最初の部分はすでに証明した．G の絶対既約通常表現 ρ を考えよう．ρ の次数を n とする．ξ を任意の $n\times n$ 行列としたとき，前と同様に，

$$\alpha=\frac{1}{g}\sum_{y\in G}\rho(y)\xi\rho(y^{-1})$$

は，すべての $x\in G$ に対し $\rho(x)\alpha=\alpha\rho(x)$ を満たすことが確かめられる．したがって定理 16.5.5 により，α は単位行列のスカラー倍 λI_n となる．ただしスカラー α は ξ に関係する．そこで $\xi=e_{rs}$ のとき $\lambda=\lambda_{rs}$ と書くことにする．すると $\lambda_{rs}\delta_{ij}=(\rho_{ir}, \rho_{sj})$ となることがわかる．一方 $(\rho_{ir}, \rho_{sj})=(\rho_{sj}, \rho_{ir})$ であるから，$i=j$ かつ $r=s$ でなければ，$\lambda_{rs}\delta_{ij}=\lambda_{ji}\delta_{sr}=0$ となる．$(\rho_{ij}, \rho_{ji})=\lambda_{ii}=(\rho_{ji}, \rho_{ij})=\lambda_{jj}$ である．ゆえに $\lambda_{11}=\lambda_{22}=\cdots=\lambda_{nn}=\lambda$ はすべての添数に対し同じ値をとる．したがって

$$\begin{aligned} n\lambda &= \sum_{j}\lambda_{jj} \\ &= \frac{1}{g}\sum_{y,j}\rho_{ij}(y)\rho_{ji}(y^{-1}) \\ &= \frac{1}{g}\sum_{y}\rho_{ii}(1) \end{aligned}$$

$$=1$$

となり，$\lambda=1/n$ である．これで定理の残りの部分が証明された．$n\lambda=1$ だから，次数nはFの標数で割れないということに注意する．

これらのことから指標に関する以下の結果が得られる．

定理 16.6.5. χ, ϕ を異なる既約指標とすると $(\chi, \phi)=0$ となる．χ が絶対既約指標ならば，$(\chi, \chi)=1$ となる．

証：χ, ϕ を既約表現 ρ, σ の指標とすると，$y\in G$ に対し $\chi(y)=\sum_i \rho_{ii}(y)$, $\phi(y)=\sum_j \sigma_{jj}(y)$ となる．スカラー積は双線形であるから，

$$(\chi, \phi)=\sum_{i,j}(\rho_{ii}, \sigma_{jj})=0$$

となる．次にχをn次の絶対既約表現ρの指標とすると，

$$(\chi, \chi)=\sum_{i,j}(\rho_{ii}, \rho_{jj})=\sum_i(\rho_{ii}, \rho_{ii})=\sum_i \frac{1}{n}=1$$

となり証明が終った．

系 16.6.2. 恒等表現に対しては $\sum_{x\in G}\chi(x)=g$ となり，恒等表現以外の既約表現に対しては $\sum_{x\in G}\chi(x)=0$ となる．

恒等表現においては，任意のxに対し $\chi(x)=1$ であるから，$\sum_{x\in G}\chi(x)=g$ となる．しかしχをそれ以外の既約表現の指標とし，ϕを恒等指標とすると，$(x, \phi)=0$ より $1/g\sum\chi(x)=0$ となる．

定理 16.6.6. χ, ϕ を指標，χ_i, $i=1, \cdots, r$ を絶対既約指標とし，$\chi=\sum a_i\chi_i$, $\phi=\sum b_i\chi_i$ と書けたとすると，$(\chi, \phi)=\sum a_ib_i$ となる．したがって体Fの標数が0のときは，指標ϕに対し，$(\phi, \phi)=1$ となることが，ϕが絶対既約指標であるための必要十分条件である．

証：スカラー積の双線形性を使うと，実質的には定理16.6.5の系である．$\phi=\sum c_i\chi_i$ とする．ただし c_i は非負整数である．このとき $(\phi, \phi)=\sum c_i^2=1$

とすると，標数0の体では1つの c_i が1で，他はすべて0である．

定理 16.6.7. 可換群Gの絶対既約表現はすべて1次である．

証：G は可換だから，各元は1つの共役類をつくり，G の位数を g とすると，g 個の絶対既約表現がある．その次数を $n_1, \cdots, n_g$ とすると，$g=n_1^2+n_2^2+\cdots+n_g^2$ が成り立つ．ゆえに $n_1=n_2=\cdots=n_g=1$ となる．そしてすべての1次表現 ρ に対し，$\chi(x)=\rho(x)$ となるから，表現は指標と一致し，実際第13章で扱った可換群の指標と同じものになる．

定理 16.6.8. xを群Gの位数mの元，ρをGのn次の表現とする．すると必要ならば1のm乗根をFにつけ加えることにより，$\rho(x)$ は対角線上に1のm乗根がならんだ対角行列に相似となる．またFが複素数体のときには $\chi(x^{-1})$ は $\chi(x)$ の複素共役 $\overline{\chi(x)}$ になる．

証：行列 $1, \rho(x), \cdots, \rho(x^{m-1})$ は位数mの巡回群Cの1つの表現になっている．しかしCの絶対既約表現は1次で，$\sigma(x)=(b)$ と書ける．ただし，$1=x^m$ だから $b^m=1$ で，b は1のm乗根である．R_C において $1/m(1+\omega x+\omega^2x^2+\cdots+\omega^{m-1}x^{m-1})$ が絶対既約表現を生じる巾等元であることが容易に分かる（ω は1のm乗根全体を動かす）．したがって1のm乗根を体F（その標数はもちろんmの約数ではない）につけ加えることにより，Cの表現 $\rho(x)$ は完全可約となり，$\rho(x)$ に相似な対角行列 diag.$(b_1, \cdots, b_n)$ が得られる．ただし各 b_i は1のm乗根である．そして $\chi(x)=b_1+\cdots+b_n$ となる．また，$\rho(x^{-1})$ は diag.$(b_1^{-1}, \cdots, b_n^{-1})$ に相似にならなければならないから，$\chi(x^{-1})=b_1^{-1}+\cdots+b_n^{-1}$ となる．そしてFが複素数体のときは1の巾根の逆数というのは複素共役な数のことであるから $b_i^{-1}=\overline{b_i}$ となり，$\chi(x^{-1})=\overline{\chi(x)}$ となる．

ρ を群Gの表現とし，各 $x\in G$ に対し $\hat{\rho}(x)=\rho(x^{-1})^T$ と定義する．ただし肩にTをつけたのは転置行列を意味する．すると，

$$\begin{aligned}\hat{\rho}(xy)&=\rho(y^{-1}x^{-1})^T=[\rho(y^{-1})\rho(x^{-1})]^T\\&=\rho(x^{-1})^T\rho(y^{-1})^T=\hat{\rho}(x)\hat{\rho}(y)\end{aligned}$$

となるから，$\hat{\rho}$ もGの表現で，**反傾表現**（contragredient representation）とよばれる．

L を ρ の表現加群とし，$u_1, \cdots, u_n$ を体 F 上の基底とする．体 F 上の基底 $v_1, \cdots, v_n$ をもつ別の空間 $\hat{L}$ をとり，$u=a_1u_1+\cdots+a_nu_n\in L$ と $v=b_1v_1+\cdots+b_nv_n\in\hat{L}$ とのスカラー積 $u\cdot v$ を

$$u\cdot v=a_1b_1+a_2b_2+\cdots+a_nb_n\in F$$

という規則で定義する．このスカラー積は $u_i\cdot v_j=\delta_{ij}$ により定義された $(L, \hat{L})$ 上の双線形関数である．

$$v_ix=\sum_j \hat{\rho}_{ij}(x)v_j=\sum_j \rho_{ji}(x^{-1})v_j$$

という規則により，$v_1, \cdots, v_n$ を $\hat{\rho}$ の表現基底にすると，$\rho(x)\rho(x^{-1})=I_n$ となることから，

$$\begin{aligned}u_ix\cdot v_jx&=\sum_{k,s} \rho_{ik}(x)\rho_{sj}(x^{-1})(u_k\cdot v_s)\\&=\sum_k \rho_{ik}(x)\rho_{kj}(x^{-1})\\&=\delta_{ij}\end{aligned}$$

となる．ゆえにすべての $u\in L$, $v\in\hat{L}$, $x\in G$ に対し $ux\cdot vx=u\cdot v$ となり，G の同じ元を両成分に作用させることはスカラー積を保存する．$\hat{L}$ の任意の部分空間 M' に対し，すべての $v\in M'$ に対し $u\cdot v=0$ となる $u\in L$ の全体がつくるLの部分空間Mを対応させよう．すると $\dim. M'+\dim. M=n$ となり，この対応はLと$\hat{L}$の部分空間の間の双対対応である．M' が$\hat{L}$の表現部分加群とすると，$v\in M'$ と $x\in G$ に対し $vx^{-1}\in M'$ となるから，すべての $v\in M'$ と $u\in M$ に対し $u\cdot vx^{-1}=0$, したがって $ux\cdot v=0$ となり，$ux\in M$ となる．よってMはLの表現部分加群である．したがって特に$\hat{L}$が既約であることはLが既約であるための必要十分条件である．ρ が $n\times n$ 絶対既約表現ならば，ρ はF上 n^2 次元だから，$\hat{\rho}$ もF上 n^2 次元で明らかに絶対既約である．

定義より $\hat{\hat{\rho}}=\rho$ となる．またρとσが同値だとすると，適当なSにより，

$$S^{-1}\rho(x^{-1})S=\sigma(x^{-1})$$

がすべての $x\in G$ に対し成り立つ．転置行列を考えると，すべての $x\in G$ に

対し

$$S^T\rho(x^{-1})^T S^{T-1}=\sigma(x^{-1})^T$$

が成り立ち，$\hat{\rho}$ と $\hat{\sigma}$ が同値になる．

G の共役類の数を r とする．$\rho_1, \cdots, \rho_r$ を G の F 上の絶対既約表現とする．ただし ρ_1 は恒等表現で，すべての $x\in G$ に対し $\rho_1(x)=1$ と約束しておく．（これは $(1/g)\sum_{x\in G} x$ という巾等元に対応している．）すると $\hat{\rho}_1=\rho_1, \cdots, \hat{\rho}_r$ は同じ表現をならべかえたものになっている．同様に $C_1, \cdots, C_r$ を G の共役類とし，$C_1=1$ は単位元だけからなる共役類と約束しておく．ある共役類 C_i の元の逆元全体はまた1つの共役類 C_i' をつくる．ゆえに $C_1'=C_1, \cdots, C_r'$ も G の共役類の全体になっている．

$\rho(x)$ の指標が $\chi(x)$ のとき，$\hat{\rho}(x)$ の指標を $\bar{\chi}(x)$ で表わすことにする．$\chi(x)=\mathrm{trace}\,\rho(x)$ であるから，

$$\bar{\chi}(x)=\mathrm{trace}\,\rho(x^{-1})^T=\mathrm{trace}\,\rho(x^{-1})=\chi(x^{-1})$$

となり，定理 16.6.8 で注意したように複素数体においては $\chi(x^{-1})$ は $\chi(x)$ の複素共役 $\overline{\chi(x)}$ になる．したがって，この記号は複素共役の記号と複素数体上では一致している．複素数体上では $\rho=\hat{\rho}$ となるのは ρ の指標 $\chi(x)$ がすべて実数となるときに限るということを注意しておく．

絶対既約表現 ρ_a の指標が共役類 C_i の元でとる値を $\chi_i{}^a$ と書くことにする．また C_i の元の数を h_i と書く．h_i というのは C_i の元 x の正規化群の指数に等しく，正規化群の位数を g_i とすれば，$g_ih_i=g$ となる．

定理 16.6.9. 群 G の絶対既約指標に関して，以下の直交関係式が成り立つ：

$$\sum_{i=1}^{r}\frac{\chi_i{}^a\overline{\chi_i{}^b}}{g_i}=\delta_{ab},$$

$$\sum_{a=1}^{r}\overline{\chi_i{}^a}\chi_j{}^a=\delta_{ij}g_j.$$

証：定理 16.6.5 により

$$\frac{1}{g}\sum_{x\in G}\chi^a(x)\chi^b(x^{-1})=\delta_{ab}$$

が成り立つ．x と y が同じ共役類 C_i にはいっていれば $\chi(x)=\chi(y)$ が成り立ち，x^{-1} と y^{-1} も同じ共役類 C_i' にはいる．そして $\chi^b(x^{-1})=\overline{\chi^b}(x)$ である．したがって上の和のうち C_i の元 x についての h_i 個の項は $\chi_i{}^a\overline{\chi_i{}^b}$ に等しい．ゆえに

$$\sum_{i=1}^{r}\frac{h_i}{g}\chi_i{}^a\overline{\chi_i{}^b}=\delta_{ab},$$

すなわち，

$$\sum_{i=1}^{r}\frac{\chi_i{}^a\overline{\chi_i{}^b}}{g_i}=\delta_{ab}$$

となる．そこで M, M' という行列を，$M=(m_{ai})$，$a, i=1, \cdots, r$，ただし $m_{ai}=\chi_i{}^a$，$M'=(r_{ib})$，$i, b=1, \cdots, r$，ただし $r_{ib}=(1/g_i)\overline{\chi_i{}^b}$ と置くと，上のことは

$$MM'=I_r$$

ということを意味し，M' は M の逆行列である．したがって，$M'M=I_r$ も成り立ち，

$$\sum_{a=1}^{r}\frac{1}{g}\chi_i{}^a\overline{\chi_j{}^a}=\delta_{ij}$$

が成り立つが，これから２番目の関係式が出る．

群環の構造を考えることにより，指標の関係式がもっと得られる．R_G の単純環への直和分解

$$R_G=R_1\boxplus\cdots\boxplus R_a\boxplus\cdots\boxplus R_r$$

において，$e_{ij}{}^a$, i, $j=1, \cdots, n$ を R_a の行列単位とすると，R_a の単位元は $e_a=e_{11}{}^a+e_{22}{}^a+\cdots+e_{nn}{}^a$ となる．R_a に付随した既約表現 $\rho_a=\rho^a$ は R_a の極小右イデアルによる表現と同値である．そこで

$$e_{11}{}^a, e_{12}{}^a, \cdots, e_{1n}{}^a$$

を基底として持つ極小イデアル $e_{11}{}^aR$ に付随しているとしよう．すると，

$$e_{1i}{}^ax=\sum_j\rho_{ij}{}^a(x)e_{1j}{}^a,\quad i=1, \cdots, n$$

となる．$x=x_1+x_2+\cdots+x_a+\cdots+x_r$，$x_a\in R_a$ とすると，

$$x_a=e_axe_a=e_ax=xe_a$$

となる．もし

$$x_a=\sum_{i,j} x_{ij}{}^a e_{ij}{}^a$$

とすると，$e_{1i}{}^a x=e_{1i}{}^a e_a x=e_{1i}{}^a x_a$ だから，

$$e_{1i}{}^a x e_{jj}{}^a=x_{ij}{}^a e_{1j}{}^a$$

となる．一方表現の定義より，

$$e_{1i}{}^a x e_{jj}{}^a=\rho_{ij}{}^a(x) e_{1j}{}^a$$

となる．ゆえに常に $x_{ij}{}^a=\rho_{ij}{}^a(x)$ が成り立ち，

$$x_a=\sum_{i,j}\rho_{ij}{}^a(x) e_{ij}{}^a$$

となる．

共役類 C_k に属する元の和 $\sum_{C_k} x$ という R_G の元のことも共役類と同じく C_k と書くことにするが，混乱することはないと思う．すると，$C_1, C_2, \cdots, C_r$ が R_G の中心 Z_G の基底をつくる．

$$C_k=C_k{}^1+\cdots+C_k{}^a+\cdots+C_k{}^r,\quad C_k{}^a\in R_a$$

とする．$C_k{}^a$ は R_a の中心にはいるから，e_a のスカラー倍である．そこで

$$C_k{}^a=u_{ka}e_a$$

とすると，

$$\mathrm{trace}\,\rho^a(C_k{}^a)=\sum_{x\in C_k}\mathrm{trace}\,\rho^a(x)$$

だから，ρ_a の次数を n_a とすると，$n_a u_k{}^a=h_k\chi_k{}^a$ となる．よって

$$u_k{}^a=\frac{h_k\chi_k{}^a}{n_a}$$

となり，

$$C_k{}^a=\frac{h_k\chi_k{}^a}{n_a}e_a$$

となる．

R_G の元 $C_1, \cdots, C_r$ は $Z(R_G)$ の基底だから，それらの積は，

$$C_jC_i=C_iC_j=\sum_k c_{ijk}C_k$$

と書けるが，標数0の体 F 上では $C_iC_j=C_jC_i$ は負の項を含まないから，c_{ijk} は非負整数となる．

R_G は単純環 R_a の直和だから，C_i の成分 $C_i{}^a$ も C_i と同じ関係式を満たす．ゆえに，

定理 16.6.10.

$$C_i{}^aC_j{}^a=C_j{}^aC_i{}^a=\sum_k c_{ijk}C_k{}^a,\quad a=1,\cdots,r$$

および，

$$\frac{h_i\chi_i{}^a}{n_a}\,\frac{h_j\chi_j{}^a}{n_a}=\sum_k c_{ijk}\frac{h_k\chi_k{}^a}{n_a},\quad a=1,\cdots,r$$

が成り立つ．

定理16.6.4の証明において，絶対既約表現の次数を $n=n_a$ とすると，$n\lambda=1$ となることがわかっていたから，定理16.6.10において n_a で割ることが許される．

体 F 上の2つの線形空間 L と M が与えられたとき，それらの**テンソル積** (tensor product) $L\times M$ を次のように定義する：$u_1,\cdots,u_m$ を L の基底，$v_1,\cdots,v_n$ を M の基底とするとき，$L\times M$ は u_iv_j, $i=1,\cdots,m$, $j=1,\cdots,n$ を基底とする F 上の線形空間で，

$$u=a_1u_1+\cdots+a_mu_m\in L,$$
$$v=b_1v_1+\cdots+b_nv_n\in M$$

のとき，$L\times M$ の元として積 $uv=\sum_{i,j}a_ib_ju_iv_j$ を定義する．また，L や M の基底を取り換えることは $L\times M$ の基底を取り換えることに対応する．

L が群 G の表現 ρ に対する F-G 加群で，M が G の表現 σ に対する F-G 加群のとき，これらの表現の**クロネッカー積** (Kronecker product) $\rho\times\sigma$ という G の $L\times M$ 上の表現を

$$(uv)x=(ux)(vx),\quad u\in L,\quad v\in M,\quad x\in G$$

で定義する．したがって，ρ_1 が ρ に同値で，σ_1 が σ に同値ならば，$\rho_1\times\sigma_1$ は $\rho\times\sigma$ に同値になる．

定理 16.6.11. ρ と σ をGの表現，その指標を χ と ψ とし，ϕ を $\rho\times\sigma$ の指標とすると，任意の $x\in G$ に対し，$\phi(x)=\chi(x)\psi(x)$ が成り立つ．

証：$u_i x=\sum_j \rho_{ij}(x)u_j,\ i=1,\cdots,m,\ v_i x=\sum_j \sigma_{ij}(x)v_j,\ i=1,\cdots,n$ とすると，

$$\chi(x)=\sum_i \rho_{ii}(x),\quad \psi(x)=\sum_i \sigma_{ii}(x)$$

となる．一方

$$(u_i v_j)x=\sum_{k,t}[\rho_{ik}(x)u_k][\sigma_{jt}(x)v_t]$$

であるから，

$$\begin{aligned}\phi(x)&=\sum_{i,j}\rho_{ii}(x)\sigma_{jj}(x)\\&=[\sum_i \rho_{ii}(x)][\sum_j \sigma_{jj}(x)]\\&=\chi(x)\psi(x)\end{aligned}$$

となる．

テンソル積およびクロネッカー積に対して可換律および結合律の成り立つことが，定義から分かる．したがって ρ_a,ρ_b がGの絶対既約表現ならば，

$$\rho_b\times\rho_a=\rho_a\times\rho_b=\sum_{c=1}^{r} g_{abc}\rho_c$$

と書ける．ただし，g_{abc} というのは $\rho_a\times\rho_b$ を既約表現の直和に分解したときの ρ_c の重複度を表わす非負整数である．指標に関しても同じ関係式が成り立つ．これを定理の形に述べると，

定理 16.6.12. 群Gの絶対既約指標は

$$\chi_i^a\chi_i^b=\sum_c g_{abc}\chi_i^c$$

という関係式を満たす．ただし g_{abc} というのはある可換結合代数の構造定数である．

いままでに分かった指標の関係式を要約しておく．$C_1=1,C_2,\cdots,C_r$ をGの共役類，$\rho_1=$恒等表現，$\rho_2,\cdots,\rho_r$ を絶対既約表現とし，a 番目の表現における i 番目の共役類の元での指標を χ_i^a と書くことにする．

	$C_1 \cdots C_i \cdots C_r$
ρ_1	$\chi_1{}^1 \cdots \chi_i{}^1 \cdots \chi_r{}^1$
	$\cdots\cdots\cdots\cdots\cdots$
ρ_a	$\chi_1{}^a \cdots \chi_i{}^a \cdots \chi_r{}^a$
	$\cdots\cdots\cdots\cdots\cdots$
ρ_r	$\chi_1{}^r \cdots \chi_i{}^r \cdots \chi_r{}^r$

そして共役類 C_i の元の数を h_i とすると，$g_i h_i = g$ が成り立っている.

1) 行について：

$$\sum_{i=1}^{r} \frac{\chi_i{}^a \overline{\chi_i{}^b}}{g_i} = \delta_{ab}.$$

2) 列について：

$$\sum_{a=1}^{r} \chi_i{}^a \overline{\chi_j{}^a} = \delta_{ij} g_i.$$

3) 各行において：

$$\frac{h_i \chi_i{}^a}{n_a} \frac{h_j \chi_j{}^a}{n_a} = \sum_k c_{ijk} \frac{h_k \chi_k{}^a}{n_a}.$$

4) 各列において：

$$\chi_i{}^a \chi_i{}^b = \sum_c g_{abc} \chi_i{}^c.$$

ただし c_{ijk}, g_{abc} はある可換結合代数の構造定数である.

群 G の置換群としての表現 $\pi(G)$ は行列表現とみなすことができる. なぜなら，$x \in G$ に対し

$$\pi(x) = \begin{pmatrix} u_1 \cdots u_n \\ u_{i_1} \cdots u_{i_n} \end{pmatrix}$$

とすると，これは基底 $u_1, \cdots, u_n$ 上の

$$u_j x = u_{i_j}$$

という表現 ρ とみなすことができ，その指標 $\chi(x)$ は $\pi(x)$ によって固定される文字の数となる.

定理 16.6.13. 位数 g の群 G の置換表現 $\pi(G)$ において，可移域の数を k とすると，$\sum_{x \in G} \chi(x) = kg$ が成り立つ. そして，この表現は行列表現としては

ちょうどk回恒等表現を含んでいる．

証：k個の可移域の文字の数を$n_1, n_2, \cdots, n_k$とする．j番目の可移域のある文字a_jを固定する部分群H_jは指数がn_jで位数はg/n_jとなる．したがってa_jはGの元でg/n_j回固定され，j番目の可移域の文字が固定される回数は$n_j \cdot g/n_j = g$となる．したがってk個の可移域全体で文字が固定される回数はkgとなり，$\sum_{x \in G} \chi(x) = kg$となる．$\chi$が絶対既約指標の和として$\chi = \sum_a m_a \chi^a$と表わされたとすると，定理16.6.5の系より$\sum_{x \in G} \chi(x) = m_1 g$となるはずだから，この表現は恒等表現を$m_1 = k$回含む．

定理 16.6.14. χを可移置換群Gの指標とすると，$\sum_{x \in G} \chi^2(x) = tg$が成り立つ．ただしある文字を固定する部分群$H$の可移域の数を$t$とする．$t$というのは$G$における両側剰余類$HxH$の数でもある．

証：Gを文字$1, 2, \cdots, n$の上の可移置換群とする．文字iを固定する部分群をH_iと置く（$i=1, \cdots, n$）．H_iはすべて共役であるから，$H=H_1$としてよい．Hの位数をhとすると，前定理により

$$\sum_{x \in H_i} \chi(x) = th$$

となる．したがって

$$\sum_i \sum_{x \in H_i} \chi(x) = tnh = tg$$

となる．ところが，左辺においてはxを含む各H_iについて1回ずつ$\chi(x)$を勘定している．そしてxは$\chi(x)$個の文字を固定するから，xは$\chi(x)$個の異なるH_iに含まれる．（xがすべての文字を動かすときは，この数は0である．）ゆえに

$$tg = \sum_i \sum_{x \in H_i} \chi(x) = \sum_{x \in G} \chi(x)^2$$

となる．またGにおける両側剰余類HxHの数がtになることが容易に分かる．なぜなら，$G = H + Hx_2 + \cdots + Hx_n$とする．ただし$H$というのは1を固定する部分群で，$x_i = (1, i, \cdots)$，$i = 2, \cdots, n$とする．もし$Hx_iH = Hx_jH$と

すると，$x_i=h_1x_jh_2$ となる $h_1, h_2\in H$ が存在する．すると h_2 は j を i に移さなければならず，したがって i と j はHの同じ可移域にはいる．逆に，i と j とがHの同じ可移域にはいったとする．すると j を i に移す $h_2\in H$ が存在し，x_jh_2 は1を i に移す．よって $x_jh_2\in Hx_i$ となり，$x_i=h_1x_jh_2$ と書け，$Hx_iH=Hx_jH$ となる．一方Hによる両側剰余類は Hx_iH のどれかに一致するから，両側剰余類 HxH の数は可移域の数に等しい．

定理 16.6.15. 群Gの複素数体上の２重可移表現は恒等表現と絶対既約表現の和である．

証：２重可移表現に対しては，文字１を固定する部分群Hは１および残りの文字全部というちょうど２つの可移域をもつから，

$$\sum \chi^2(x)=2g$$

となる．$\chi(x)$ は実数だから，

$$\sum_{x\in G}\chi(x)\overline{\chi(x)}=2g$$

と書くこともできる．そして χ が絶対既約指標の和として $\chi=\sum_a c_a\chi^a$ と表わされているとすると，直交関係式より

$$\sum_{x\in G}\chi(x)\overline{\chi(x)}=\sum_x\left[\sum_a c_a\chi^a(x)\right]\left[\sum_a c_a\overline{\chi_a(x)}\right]=g\sum_a c_a{}^2$$

となる．ゆえに $\sum_a c_a{}^2=2$ となり，すでに $c_1=1$ となることが分かっていたから，あと１つだけ $c_a=1$ となる．

16.7. 非原始的表現

群 G の表現加群Mが部分空間 $M_1, M_2, \cdots, M_n$ の直和になり，各 M_i の上で表現が**可移**（transitive）かつ**非原始的**（imprimitive）だとする．すなわち

1） 任意の M_i と M_j に対し

$$M_ix=M_j$$

となる $x\in G$ が存在する．

2） 任意の M_i と任意の $x\in G$ に対し

$$M_i x = M_j$$

となる M_j が存在する．最初の方が可移性で，２番目が非原始性である．

特定の部分空間 M_1 を選ぶ．$M_1 x = M_1$ となる x の全体は単位元 1 を含んでいるから空集合ではなく，G の部分群 H をつくることが容易に分かる．したがって $h \in H$ ならば

$$M_1 h = M_1$$

となり，M_1 は H の表現加群となる．

$$M_1 b_i = M_i$$

となる $b_i \in G$ をとっておくと，$M_1 x = M_i$ となる x の全体は剰余類 Hb_i となるから，

$$G = H + Hb_2 + Hb_3 + \cdots + Hb_n$$

となる．そして

$$M_1(hb_i) = M_i, \quad i = 1, \cdots, n$$

だから，これにより部分空間と H の左剰余類の対応ができた．

$$M_i x = M_i$$

とすると，

$$M_1 b_i x = M_1 b_i$$

したがって

$$M_1 b_i x b_i^{-1} = M_1$$

となるから，$b_i x b_i^{-1} \in H$，すなわち $x \in b_i^{-1} H b_i$ となり，x は H に共役な群に含まれる．最後に，もし

$$M_i x = M_j$$

とすると，

$$x \in b_i^{-1} H b_j$$

となる．M_1 の基底 $v_1, \cdots, v_m$ に付随する H の表現を ρ_1 とする．すると M_i の基底として $v_1 b_i, \cdots, v_m b_i$ をとることができる．任意の $x \in G$ に対し

$$M_1 x = M_{j_1}, \cdots, M_i x = M_{j_i}, \cdots, M_n x = M_{j_n}$$

となる．ただし，$M_{j_1}, \cdots, M_{j_n}$ に x^{-1} を作用させると $M_1, \cdots, M_n$ となるか

ら，これらは $M_1, \cdots, M_n$ の置換である．そして $M_i x = M_j$ $(j = j_i)$ とすると，$x \in b_i^{-1} H b_j$，すなわち $b_i x b_j^{-1} = h_{ij} \in H$ となる．ゆえに M_i の基底として $v_k b_i$，$k = 1, \cdots, m$ をとると

$$v_k b_i \cdot x = (v_k \cdot h_{ij}) b_j, \quad k = 1, \cdots, m$$

となる．いいかえると，M による表現のうち M_i による部分は h_{ij} の M_1 上の表現

$$v_k (b_i x b_j^{-1}) = v_k h_{ij}$$

により完全に決まるわけである．ゆえに $y \notin H$ ならば $\rho_1(y) = 0$ と約束すると，

$$\rho(x) = (\rho_1(b_i x b_j^{-1})) \qquad i, j = 1, \cdots, n$$

となる．そして $\rho(x)$ というのは m 次の行列 n^2 個からなる mn 次の行列である．したがって部分空間 $M_1, \cdots, M_n$ 上可移かつ非原始的な表現はすべて G の指数 n の部分群 H の表現 ρ_1 により決まってしまう．逆も成り立つ．

$$G = H + Hb_2 + \cdots + Hb_n$$

とし，ρ_1 を H の任意の表現とする．$y \notin H$ ならば $\rho_1(y) = 0$ と約束し，

$$\rho(x) = (\rho_1(b_i x b_j^{-1})) \qquad i, j = 1, \cdots, n$$

と定義する．すると，行列の積をブロックにわけて計算すると，

$$\begin{aligned}\rho(x)\rho(y) &= (\rho_1(b_i x b_j^{-1}))(\rho_1(b_k y b_t^{-1})) \\ &= (\rho_1(b_i x b_j^{-1}) \rho_1(b_j y b_t^{-1})) \\ &= (\rho_1(b_i x y b_t^{-1})) \\ &= \rho(xy)\end{aligned}$$

となり，また明らかに

$$\rho(1) = (\rho_1(b_i 1 b_i^{-1})) = (\rho_1(1)) = I$$

となる．したがって $\rho(x)$ は G の表現になる．

定理 16.7.1. 群 G の部分群 H の m 次の表現 ρ_1 が与えられ，$G = H + Hb_2 + \cdots + Hb_n$ とする．$y \notin H$ のとき $\rho_1(y) = 0$ と約束すれば，

$$\rho(x) = (\rho_1(b_i x b_j^{-1})) \qquad i, j = 1, \cdots, n$$

はGの mn 次の表現で，その表現加群 M は $H, Hb_2, \cdots, Hb_n$ に対応する部分空間 $M_1, M_2, \cdots, M_n$ を持ち，ρ は $M_1, \cdots, M_n$ の上に可移かつ非原始的となる．逆に表現加群の部分空間上に可移かつ非原始的となる表現はすべてこのようにして得られる．

証：$u_1, \cdots, u_m, \cdots, u_{mn}$ を定理における ρ の表現加群の基底とすると，$u_1, \cdots, u_m$ が H の表現 ρ_1 に対する基底で，$u_{m(i-1)+j}=u_jb_i$, $i=1, \cdots, n$ となる．したがって基底 $u_1, \cdots, u_{mn}$ を持つ加群 M の適当な部分空間 $M_1, \cdots, M_n$ 上に ρ が可移かつ非原始的となる．

G の表現 ρ は H の表現 ρ_1 により**誘導された**（induced）という．

系 16.7.1. H の表現 ρ_1 により誘導された G の表現 ρ は G における H の剰余類の代表系の選び方に関係しない．

これは代表系を変えても部分空間 $M_1, \cdots, M_n$ は変わらず，ただそれらの基底がかわるだけであるということから分かる．

定理 16.7.2. H の表現 ρ_1 により誘導された G の表現を ρ とし，ρ_1, ρ の指標を χ_1, χ とする．G の共役類 C_j の元の数を h_j とし，$g=g_jh_j$ とする．ただし G の位数を g, H の位数を h とする．このとき，$x\in C_j$ ならば

$$\chi(x)=\frac{g_j}{h}\sum_{z\in C_j\cap H}\chi_1(z)$$

となる．

証：$w\notin H$ ならば $\chi_1(w)=0$ と約束すれば，$\chi(x)=\sum_{i=1}^{n}\chi_1(b_ixb_i^{-1})$ となる．よって

$$\chi(x)=\frac{1}{h}\sum_{y\in G}\chi_1(yxy^{-1})$$

となる．なぜなら，Hb_i のすべての元 y は，右辺において同じ値 $\chi_1(b_ixb_i^{-1})$ をとるからである．そして y が G 全体を動くとき，yxy^{-1} は C_j を動き，各 $z\in C_j$ をちょうど g_j 回通る．よって

$$\sum_{y\in G}\chi_1(yxy^{-1})=g_j\sum_{z\in C_j\cap H}\chi_1(z)$$

となり，定理が証明された．

定理16.7.3.（相反定理）． ρ, ρ_1 をそれぞれ群 G，およびその部分群 H の標数0の体上の絶対既約表現とする．このとき ρ を H に制限した表現における ρ_1 の重複度は，ρ_1 により誘導された G の表現 ρ^* における ρ の重複度に等しい．

証：$\chi=\chi^a$ を ρ の指標，$\chi_1=\chi_1{}^c$ を ρ_1 の指標，χ^* を ρ^* の指標とする．χ^* が G の既約指標 χ^b により $\chi^*=\sum_b m_b\chi_b$ と書けたとし，χ は H に制限したとき，H の既約指標 $\chi_1{}^d$ により，$\chi=\chi^a=\sum_d n_d\chi_1{}^d$ と書けたとする．すると ρ^* における ρ の重複度は m_a, ρ を H に制限したものにおける ρ_1 の重複度は n_c である．前定理により，

$$\frac{1}{g_j}\chi_j{}^*=\frac{1}{g_j}\sum_b m_b x_j{}^b=\frac{1}{h}\sum_{z\in C_j\cap H}\chi_1{}^c(z)$$

となる．ただし空集合上の和は0と約束しておく．両辺に $\overline{\chi_j{}^a}$ を掛け，j について加えると

$$\sum_{j,b}m_b\frac{\overline{\chi_j{}^a}\chi_j{}^b}{g_j}=\frac{1}{h}\sum_j\overline{\chi_j{}^a}\sum_{z\in C_j\cap H}\chi_1{}^c(z)$$

となり，G および H における直交関係を使うと，

$$\begin{aligned}m_a&=\frac{1}{h}\sum_{d,j}n_d\overline{\chi_{1,j}{}^d}\sum_{z\in C_j\cap H}\chi_1{}^c(z)\\&=\frac{1}{h}\sum_{d,z\in H}n_d\overline{\chi_1{}^d}(z)\chi_1{}^c(z)\\&=\frac{1}{h}hn_c\\&=n_c\end{aligned}$$

となり，これが定理でいっていることである．

16.8. 指標理論のいくつかの応用

この節では，体Fというのは複素数体のことにするが，表現される群Gの位数を体の標数が割らなければ成り立つ結果もいくつかある．

まず代数的数に関するいくつかの事実が必要になる*)．数θは，モニックな多項式[1]

$$x^n+a_1x^{n-1}+\cdots+a_n=0$$

の根 $x=\theta$ となるとき，**代数的数**（algebraic number）とよばれる．ただし，$a_1, \cdots, a_n$ は有理数である．$a_1, \cdots, a_n$ が有理整数のとき，θ は**代数的整数**（algebraic integer）とよばれる．

定理 16.8.1. 代数的整数である有理数は，有理整数である．

証：$\theta=r/s$ を既約な有理数で，

$$x^n+a_1x^{n-1}+\cdots+a_n=0$$

を満たすとする．ただし $a_1, \cdots, a_n$ は整数である．すると

$$r^n=-s(a_1r^{n-1}+a_2sr^{n-2}+\cdots+a_ns^{n-1})$$

となり，sを割る任意の素数は r^n，したがってrを割らなければならない．これは r/s が既約だとしたことに反するから，$s=1$ でなければならない．したがって $\theta=r$ は有理整数である．

定理 16.8.2. 代数的数の全体は体をつくる．2つの代数的整数の和や積は代数的整数である．

証：θ を $x^n+a_1x^{n-1}+\cdots+a_n=0$ を満たす代数的数，ϕ を $x^m+b_1x^{m-1}+\cdots+b_m=0$ を満たす代数的数とする．

$$v_{i,j}=\theta^i\phi^j,\quad i=0, \cdots, n-1,\quad j=0, \cdots, m-1$$

と置くと，

---

*) これらは Birkhoff-MacLane [1] 410—422 頁に書かれている．

1) 最高次の係数が1である多項式のこと．

$$\theta v_{i,j}=v_{i+1,j},\quad i=0,\cdots,n-2$$

および

$$\theta v_{n-1,j}=-a_1v_{n-1,j}-\cdots-a_nv_{0,j}$$

が成り立つ．同様に

$$\phi v_{i,j}=v_{i,j+1},\quad j=0,\cdots,m-2$$

および

$$\phi v_{i,m-1}=-b_1v_{i,m-1}-\cdots-b_mv_{i,0}$$

が成り立つ．

補題 16.8.1. $y_1,\cdots,y_N$ のうち少なくとも1つは0でないとし，

$$zy_i=\sum_j a_{ij}y_j \qquad i=1,\cdots,N$$

が成り立っているとする．このときすべての a_{ij} が有理数ならば，z は代数的数である．もし a_{ij} がすべて整数ならば，z は代数的整数である．

証：仮定より次のような方程式系が得られる．

$$\begin{gathered}(a_{11}-z)y_1+a_{12}y_2+\cdots+a_{1N}y_N=0,\\ a_{21}y_1+(a_{22}-z)y_2+\cdots+a_{2N}y_N=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ a_{N1}y_1+a_{N2}y_2+\cdots+(a_{NN}-z)y_N=0.\end{gathered}$$

これを y_i に関する一次方程式とみたとき，少なくとも1つの y_i は0でないような解 $y_1,\cdots,y_N$ を持つ．ゆえに係数行列の行列式は0でなければならない．よって

$$\begin{vmatrix} a_{11}-z, & a_{12},\cdots, & a_{1N}\\ a_{21}, & a_{22}-z,\cdots, & a_{2N}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots\\ a_{N1}, & \cdots\cdots, & a_{NN}-z\end{vmatrix}=0$$

となる．そしてこれを展開すると，

$$(-1)^Nz^N+p_1z^{N-1}+\cdots+p_N=0$$

となる．ここで p_k は a_{ij} の整数係数多項式である．ゆえに a_{ij} がすべて有理

数ならば z は代数的数で，a_{ij} がすべて整数ならば，z は代数的整数となる．

この補題を使って定理を証明することにする．θ または ϕ が0という自明な場合は除くことにする．$y_1, \cdots, y_N$ として $v_{i,j}$ をとろう．$v_{0,0}=1$ だから $v_{i,j}$ の中に0でないものがある．そして z としては $\theta+\phi$ または $\theta\phi$ をとる．すると補題の a_{ij} としては $a_1, \cdots, a_n$ および $b_1, \cdots, b_m$ の整数係数多項式がとれる．ゆえに $z=\theta+\phi$ および $z=\theta\phi$ は代数的数となり，代数的整数の和および積は代数的整数となる．最後に，θ が $z^n+a_1z^{n-1}+\cdots+a_n=0$ を満たす0でない代数的数とすると，必要ならば z の巾で割ることにより，定数項 $a_n\neq 0$ とできる．すると $1/\theta$ は

$$w^n+\frac{a_{n-1}}{a_n}w^{n-1}+\cdots+\frac{1}{a_n}=0$$

という方程式を満たす．明らかに，$-\theta$ は $z^n-a_1z^{n-1}+\cdots+(-1)^n a_n=0$ を満たす．ゆえに代数的整数の全体は整域をつくり，代数的数の全体は体をつくる．

定理 16.8.3. 任意の指標 $\chi(x)$ は代数的整数である．定理16.6.10にでてきた $h_i\chi_i{}^a/n_a$ という数は代数的整数である．

証：1の m 乗根は $x^m-1=0$ を満たすから代数的整数である．そして定理16.6.8により任意の指標 $\chi(x)$ は1の巾根の和だから代数的整数である．定理16.6.10の c_{ijk} は整数だから，y_i として

$$\frac{h_i\chi_i{}^a}{n_a}=\eta_i{}^a,\quad i=1,\cdots,r$$

をとり，またこれらのうちの任意の1つを z としてとって，補題16.8.1を適用すると，$\eta_i{}^a$ が代数的整数となることが分かる．

定理 16.8.4. 有限群 G の絶対既約表現の次数 n_a は G の位数 g の約数である．

証：直交関係式より

$$\sum_{i=1}^{r} \frac{\chi_i{}^a \overline{\chi_i{}^a}}{g_i} = 1$$

となるが，$g_i h_i = g$ だから，

$$\sum_{i=1}^{r} \frac{\chi_i{}^a h_i \overline{\chi_i{}^a}}{g} = 1,$$

すなわち

$$\sum_{i=1}^{r} \frac{h_i \chi_i{}^a}{n_a} \overline{\chi_i{}^a} = \frac{g}{n_a}$$

となる．ところが左辺は代数的整数の積の和であるから，g/n_a も代数的整数であるが，有理数であるから，有理整数となる．ゆえに n_a は g を割り切る．

代数的整数を扱うためには，対称関数の理論が少し必要になる．

$$(z-x_1)(z-x_2)\cdots(z-x_n)$$
$$= z^n - E_1 z^{n-1} + E_2 z^{n-2} - \cdots + (-1)^n E_n$$

と展開すると，

$$E_1 = \sum x_i,$$
$$E_2 = \sum x_i x_j$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$E_r = \sum x_{i_1} x_{i_2} \cdots x_{i_r},$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$E_n = x_1 x_2 \cdots x_n$$

となる．そして明らかに $E_1, \cdots, E_n$ は $x_1, \cdots, x_n$ の任意の置換により不変であって，$x_1, \cdots, x_n$ の**基本対称式**とよばれる．体F上の多項式 $P(x_1, \cdots, x_n)$ は，$x_1, \cdots, x_n$ の置換全体のつくる対称群によって不変のとき，**対称式** (symmetric function) とよばれる．

定理 16.8.5. 任意の対称式 $P(x_1, \cdots, x_n)$ は基本対称式 $E_1, \cdots, E_n$ の多項式 $Q(E_1, \cdots, E_n)$ で，その係数が P の係数の整数係数多項式であるようなものとして表わせる．

証：Pが対称式ならば，各次数の項もそれぞれ対称式になっている．1次の

対称式は cE_1, $c \in F$ だけだから，この場合には明らかに定理は成り立っている．さらに，Pはある1つの項，たとえば

$$c(x_1 \cdots x_r)^a (x_{r+1} \cdots x_{r+s})^b \cdots (x_{u+1} \cdots x_{u+v})^t$$

の対称多項式の和になっている．ただし巾については，$a>b>\cdots>t$ と単調に減っているとする．したがって

$$K = \sum (x_1 \cdots x_r)^a (x_{r+1} \cdots x_{r+s})^b \cdots (x_{u+1} \cdots x_{u+v})^t$$

という対称和で，$a>b>\cdots>t$ となっているものについて定理を証明すればよい．次の（1），（2），（3），の順に帰納法を行なうことにする．（1）Kの次数；（2）aの値；（3）rの値．$x_1, \cdots, x_n$ がすべての項に現われるならば，E_n をくくり出すと，残りはもっと次数の低い対称式になる．したがって $u+v<n$ と仮定してよい．$a=1$ ならば $K=E_r$ である．それ以外の場合には

$$\sum x_1 \cdots x_r \cdot \sum (x_1 \cdots x_r)^{a-1} (x_{r+1} \cdots x_{r+s})^b \cdots (x_{u+1} \cdots x_{u+v})^t = E_r \cdot K^*$$

を考える．$E_r \cdot K^* = K +$(他の項) で，K^* も他の項もこの帰納法においてKよりも前にある．よって定理が証明された．

代数的数θを根として持つ最小次数の有理数係数多項式はθの**最小多項式** (minimal polynomial) とよばれる．

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

を最小多項式とすると，これはθを根として持つ任意の有理数係数多項式を割り切る．$\theta = \theta_1$ として

$$f(x) = (x-\theta_1)(x-\theta_2)\cdots(x-\theta_n)$$

となるとき，$\theta_1, \cdots, \theta_n$ をθの**共役** (conjugate) という．したがってθの満たす任意の有理数係数多項式はθの共役も満たす．よってθが代数的整数ならば，θの共役も代数的整数で，θの最小多項式の係数はθの共役の対称式であるから，代数的整数，したがって有理整数である．

表現論においては，大抵の場合1の巾根が問題になる．1の原始m乗根は $\omega = \exp(2\pi i/m)$ および $(j, m)=1$ のときの ω^j である．ωおよび他の1の原始m乗根は $x^m-1=0$ を満たし，$0<r<m$ なるrについては $x^r-1=0$ を満たさない．1のm乗根のうち残りのものは，dがmの約数を動くとき，x^d-1

$=0$ という方程式のどれかを満たす．x^m-1 から x^d-1 と共通に持つ因子を除いた $f(x)$ は1の原始 m 乗根だけを根にもつ．すなわち，

$$f(x)=\prod_j (x-\omega^j) \qquad (j, m)=1$$

で，$f(x)$ は有理整数係数で $\phi(m)$ 次である．ただし ϕ というのは Euler 関数である．実は $f(x)$ は既約になるのだが，代数的数についてここで証明することよりも，もっと進んだ理論を使わないと，このことを証明するのは困難である．我々は原始 m 乗根の基本対称式が有理整数であることがわかればよい．

定理 16.8.6. ρ_a を G の n 次の絶対既約表現とし，$(h_i, n)=1$ となる共役類 C_i があったとする．すると（1）$\chi_i{}^a=0$，または（2）$\chi_i{}^a=n\omega$ となる．ただし ω は1の巾根で，C_i は ρ_a の中心にはいる．

証：特定の $x\in C_i$ に対しては，$\rho_a(x)$ が対角行列になるように ρ_a を変換することができる．$\rho_a(x)$ の n 個の固有値がすべて等しく，たとえば1の m 乗根 ω だったとすると，

$$\rho_a(x)=\omega I_n, \quad \chi(x)=n\omega$$

となり，x は ρ_a の中心にはいる．これは定理の2番目の場合である．したがって，x の固有値の中に等しくないものがあるとき，定理の仮定があれば $\chi(x)=0$ となることをいわなければならない．この場合，x の位数は m だから，$\chi_i{}^a=\chi(x)=\omega^{e_1}+\cdots+\omega^{e_n}$ と書け，ω^{e_i} の偏角の中に等しくないものがあるから，$|\chi_i{}^a|<n$ となる．そして

$$\frac{h_i\chi_i{}^a}{n}$$

は代数的整数で，$(h_i, n)=1$ だから，$rh_i+sn=1$ となる整数 r, s が存在する．よって

$$r\left(\frac{h_i\chi_i{}^a}{n}\right)+s\cdot\chi_i{}^a=\frac{\chi_i{}^a}{n}$$

は代数的整数である．そして

$$\left|\frac{\chi_i{}^a}{n}\right|<1$$

で,

$$\xi = \frac{\chi_i{}^a}{n} = \frac{\omega^{e_1} + \cdots + \omega^{e_n}}{n}$$

である. ω をその共役 ω^j で置き換えると,

$$\prod_{(j,n)=1} [z - q(\omega^j)]$$

という係数が ω の共役の対称式, したがって有理数係数の多項式が得られる. したがって ξ の共役は

$$\frac{\omega^{je_1} + \cdots + \omega^{je_n}}{n}$$

という数のどれかである. ξ の任意の共役 $\xi^{(i)}$ は代数的整数で, $|\xi^{(i)}| \leq 1$ が成り立つ. そして $|\xi| = |\xi^{(1)}| < 1$ だから, ξ の共役全部について積をつくると, $|\xi^{(1)} \cdots \xi^{(s)}| < 1$ となる. これは有理整数であるから 0 でなければならない. したがって $\xi^{(1)} \cdots \xi^{(s)} = 0$ となり, 少なくとも 1 つの共役は 0 である. ところが, 0 の共役は 0 だけだから, $\xi = \xi^{(1)} = 0$ となり,

$$\xi = \frac{\chi_i{}^a}{n} = 0,$$

したがって $\chi_i{}^a = 0$ となるが, これが証明すべきことだった.

定理 16.8.7.[*] (1) 群 G のある共役類 C_i の元の数 h_i が素数巾だったとすると, G は単純群ではない. もっと正確にいうと, C_i の元が中心にはいるような G の準同型像が存在する. (2) p, q を素数とするとき, 位数 $p^a q^b$ の群は可解である.

証: (1) G の絶対既約表現の次数を $n_1 = 1, n_2, \cdots, n_r$ とする. C_i の元の数を $h_i = p^s$ とする. G の正則表現については, $x \in C_i$ ならば $x \neq 1$ だから, $\chi(x) = 0$ となる. 一方, 正則表現の分解により

$$\chi(x) = \sum_{a=1}^{r} n_a \chi_i{}^a$$

---

[*] W. Burnside [2] 322—323 頁参照.

となる．ここで $n_1\chi_i^1=1$ である．残りの項については，もし $p\nmid n_a$ ならば，定理 16.8.6 により，$\chi_i^a=0$ となるか C_i が準同型写像 $\rho_a(G)$ の中心にはいる．そして，$p\nmid n_a$ ならばつねに $\chi_i^a=0$ となったとすると，

$$0=1+\sum_{a=2}^{r} n_a\chi_i^a=1+p\alpha$$

となる．ただし α は代数的整数である．すると，$-(1/p)$ が代数的整数となり，矛盾である．ゆえに C_i が $\rho_a(G)$ の中心にはいるような ρ_a が存在する．

（2）Gを位数 p^aq^b の群とする．p-群は可解だから，このような群の位数に関する帰納法で証明することにする．Sylow q-部分群の中心の元は，G の中心にはいるか，p 巾個の共役元をもつ．いずれにしてもGは真正規部分群Hを持ち，帰納法の仮定からHも G/H も可解となるから，G 自身可解である．

定理 16.8.8.（Frobenius） Gをn次の可移置換群で，単位元以外はたかだか一点しか固定しないとする[1]．このとき，Gの単位元とすべての点を動かす置換の全体は，位数nの正規部分群をつくる．

証：Gを $1,2,\cdots,n$ 上の置換群とし，i を固定する部分群を H_i とする．仮定より $i\neq j$ ならば $H_i\cap H_j=1$ となる．$H=H_1$ の位数を h とすると，H_i はすべて位数が h で，H_i に属する元 $x\neq1$ は $(h-1)n$ 個ある．$[G:H]=n$ だから，G の位数は hn である．したがって残りは n 個となり，それは単位元と $n-1$ 個のすべての文字を動かす元である．

ψ を H の絶対既約指標，ψ' を ψ からつくった G の誘導指標とする．置換群Gは自然な置換表現をもっているが，その指標は $\theta_1=\psi_1'$ である．ただし ψ_1 は H の単位指標である．定理 16.6.13 により θ_1 は G の単位指標と別の指標，たとえば θ との和になっている．Gの正則表現の指標を r_G と書くことにし，$\omega=r_G-h\theta$ とおく．ω がGの指標であることを示せば定理が証明される．下の指標の表において，x は H_i の 1 と異なる元，y はすべての文字を動かす元である．

[1] このような群は一点を固定する部分群が単位元だけではないとき Frobenius 群とよばれる．

	1	x	y
ψ'	$mn,$	$\psi(x),$	0
θ	$n-1,$	$0,$	-1
r_G	$nh,$	$0,$	0
ω	$h,$	$0,$	h

ψ', θ, r_G は指標であることがわかっている．もし ω が指標ならば $\omega(1)=h$ であるから，ω は h 次の表現の指標である．$\omega(y)=h$, $\omega(x)=0$ だから，y は単位行列で表現されるが，x はそうではない．ゆえに ω は1とすべての文字を動かす元 y の全体を核とする表現である．単位元と $n-1$ 個のすべての文字を動かす元は準同型の核であるから，G の正規部分群をつくる．

そこで ω が指標であることを証明しよう．H の共役類の数を s とし，H の絶対既約指標を $\psi^a, a=1, \cdots, s$, その次数を m_a とする．すると，

$$r_H=\sum_{a=1}^{s} m_a\psi^a$$

となるが，一方 $r_G=(r_H)'$ で，$h=\sum_a m_a{}^2$ である．よって

$$\omega=\sum_a m_a[(\psi^a)'-m_a\theta]$$

となる．ゆえに任意の $\psi=\psi^a$, $m=m_a$ に対し，$\psi'-m\theta$ が G の指標であることを証明すればよい．

$$(\psi'-m\theta, \psi'-m\theta)=(\psi', \psi')-2m(\psi', \theta)+m^2(\theta, \theta)$$

となるが，$g=nh$ だから，前の指標の表から

$$(\psi', \psi')=\frac{m^2n}{h}+\frac{1}{nh}\sum_{x\neq 1}\psi(x)\overline{\psi(x)}$$

$$=\frac{m^2n}{h}+\frac{1}{h}\sum_{\substack{x\in H\\ x\neq 1}}\psi(x)\overline{\psi(x)}$$

となる．ところが

$$\sum_{x\in H}\psi(x)\overline{\psi(x)}=h$$

だから，

$$(\psi', \psi')=[m^2n+(h-m^2)]/h$$

となる．同様に上の表から，$(\psi', \theta)=m(n-1)/h$，および

$$(\theta, \theta)=[(n-1)^2+(n-1)]/nh=(n-1)/h$$

となることが分かる．ゆえに

$$(\psi'-m\theta, \psi'-m\theta)=1$$

となる．ところが，いずれにせよ，$\psi'-m\theta$ は指標の整数係数一次結合で，たとえば $\psi'-m\theta=\sum c_a\chi^a$ と表わされ，そのとき

$$(\psi'-m\theta, \psi'-m\theta)=\sum c_a^2$$

となる．ゆえに $\sum c_a^2=1$ で，ただ一つの $c_a=\pm1$ で，残りは0である．ゆえに $\psi'-m\theta=\pm\psi^a$ となる．ところが $(\psi'-m\theta)(1)=m>0$ だから，$\psi'-m\theta=\psi^a$ はGの指標である．これで $\psi'-m\theta$ が指標であることが証明され，ω は指標となるから，定理が証明された．

16.9. ユニタリ表現と直交表現

任意の $n\times n$ 行列

(16.9.1) $$A=(a_{ij})\qquad i, j=1, \cdots, n$$

に対し，双線形形式

(16.9.2) $$B(y, x)=\sum_{i,j} a_{ij}y_ix_j,\quad i, j=1, \cdots, n$$

を付随させることができる．逆にこの双線形形式に対し行列Aを付随させることもできる．双線形形式における x_j や y_i に線形変換を施したときに，対応する行列にどのような影響があるかということに興味がある．

(16.9.3) $$x_j=\sum_k c_{jk}x_k'\qquad j, k=1, \cdots, n,$$

$$y_i=\sum_s d_{is}y_s'\qquad i, s=1, \cdots, n$$

と置こう．すると

(16.9.4) $$B(y, x)=B'(y', x')=\sum_{i,j,k,s} d_{is}a_{ij}c_{jk}y_s'x_k'$$

となる．したがって $B'(y', x')$ は

(16.9.5) $$A'=D^TAC,\quad D=(d_{is}),\quad C=(c_{jk})$$

に対応することが分かる．

最も一般の双線形形式ではなく，ある種の特別なものにしか関心はない．この節においては，行列の係数は複素数とする．

(16.9.6) $$a_{ji}=\overline{a_{ij}},\quad i,j=1,\cdots,n$$

のとき，行列 A は**エルミート行列**（Hermitian matrix）という．ただし $\overline{a_{ij}}$ は a_{ij} の複素共役である．つまりエルミート行列というのは**エルミート形式**（Hermitian form）

(16.9.7) $$H(\bar{x},x)=\sum_{i,j}a_{ij}\bar{x}_i x_j,\quad a_{ij}=\overline{a_{ji}},\quad i,j=1,\cdots,n$$

に付随している．エルミート形式やエルミート行列においては，$\overline{a_{ii}}=a_{ii}$ という係数は実数であることに注意する．実エルミート行列というのは実対称行列で，実２次形式

(16.9.8) $$Q(x)=\sum_{i,j}a_{ij}x_i x_j,\quad a_{ji}=a_{ij},\quad i,j=1,\cdots,n$$

に対応している．エルミート形式（または２次形式）を不変にする正則線形変換の全体は明らかに群をつくる．ただし $\bar{x}_i$ に変換を施すと，x_i に施したものの共役に行くとする．

定　義：

(16.9.9) $$\bar{U}^T I U=I$$

を満たす行列 U は**ユニタリ行列**（unitary matrix）とよばれる．

定　義：

(16.9.10) $$V^T I V=I$$

を満たす行列 V は**直交行列**（orthogonal matrix）とよばれる．

ユニタリ行列や直交行列は正則行列であって，それらの全体がそれぞれ群をつくることは直ちに分かる．ユニタリ行列の全体は，$\bar{x}_1x_1+\cdots+\bar{x}_nx_n$ を不変にする線形変換の全体のつくる群で，直交行列の全体は，$x_1^2+\cdots+x_n^2$ を不変にする線形変換の全体のつくる群である．実ユニタリ行列は直交行列であるが，直交行列は実行列とは限らない．たとえば

(16.9.11)
$$V=\begin{pmatrix} i, & \sqrt{2} \\ -\sqrt{2}, & i \end{pmatrix}$$

も（16.9.10）を満たす．しかし，以後単に直交行列といえば実行列を意味することにする．

群の表現 $\rho(g)$ は，行列 $\rho(g)$, $g\in G$ がすべてユニタリ行列のときに**ユニタリ表現**（unitary representation），$\rho(g)$, $g\in G$ がすべて直交行列のときに**直交表現**（orthogonal representation）という．

定理 16.9.1. 有限群 G の複素数（実数）体上の任意の表現は，ユニタリ（直交）表現と同値になる．

証：エルミート形式

(16.9.12)
$$H(\bar{x}, x)=\sum a_{ij}\bar{x}_i x_j,\quad a_{ji}=\overline{a_{ij}}$$

において，x_i が複素数値をとるとき，H は実数を表わす．なぜなら，（16.9.12）の項を

(16.9.13)
$$a_{ji}\bar{x}_j x_i+a_{ij}\bar{x}_i x_j=\overline{a_{ij}}\bar{x}_j x_i+a_{ij}\bar{x}_i x_j$$

のように組み合わせると，これは複素数とその共役の和であるから実数となるし，対角項 $a_{ii}\bar{x}_i x_i$ はもちろん実数である．$H(\bar{x}, x)$ は，すべての変数が 0 のときに限り 0 となって，それ以外のときは正の数を表わすとき，**正定値**（positive definite）であるという．明らかに，正定値であるという性質は変数を正則行列で変換しても変わらない．単位行列に付随する正定値形式は

(16.9.14)
$$I(\bar{x}, x)=\bar{x}_1 x_1+\cdots+\bar{x}_n x_n$$

である．$x_j=0$ でなければ，$\bar{x}_j x_j$ は正であるから，$I(\bar{x}, x)$ は正定値である．

補題 16.9.1. n 変数の正定値エルミート形式 $H(\bar{x}, x)$ は，$\bar{x}_1 x_1+\cdots+\bar{x}_n x_n$ に変換できる．

$$H(\bar{x}, x)=\sum_{i,j} a_{ij}\bar{x}_i x_j,\quad a_{ji}=\overline{a_{ij}}$$

が正定値ならば，対角係数 a_{rr} はすべて正であることに注意する．なぜなら，$a_{rr}\leq 0$ とすると，$x_r=1$, $j\neq r$ ならば $x_j=0$ と置くと，$H(\bar{x}, x)=a_{rr}\leq 0$ と

なり，正定値であるという性質に反するからである．そこで

(16.9.15) $$H=\sum_{i,j} a_{ij}\bar{x}_i x_j,\ a_{ji}=\overline{a_{ij}},\quad i, j=1, \cdots, n$$

において

(16.9.16) $$x_1'=\sqrt{a_{11}}\left(x_1+\frac{a_{12}x_2}{a_{11}}+\cdots+\frac{a_{1n}x_n}{a_{11}}\right),$$

$$x_j'=x_j,\quad j=2, \cdots, n$$

と置こう．a_{11} は正の実数だから，この変換をすることは許される．すると

(16.9.17) $$H=\overline{x_1'}x_1'+\sum b_{ij}\overline{x_i'}x_j',\qquad i, j=2, \cdots, n$$

という形になり，$x_2', \cdots, x_n'$ に関する項は正定値形式であることが，容易な計算により分かる．これを続ければ，結局，Hを

(16.9.18) $$H=\bar{x}_1x_1+\cdots+\bar{x}_nx_n$$

という形に変換でき，補題が証明された．もしHが最初から実２次形式Qだったとすると，上と同じ操作により，Q は $x_1^2+\cdots+x_n^2$ に変換されることを注意しておく．

そこで $\rho(g), g\in G$ を有限群Gのn次の複素表現とし，Gの元を $g_1=1, g_2, \cdots, g_t$ とする．すると

(16.9.19) $$M=I+\overline{\rho(g_2)}^T I\rho(g_2)+\cdots+\overline{\rho(g_t)}^T I\rho(g_t)$$

において，各項が正定値エルミート形式に対応しているから，M自身正定値エルミート形式に対応する行列である．さらに，任意の $g\in G$ に対して

(16.9.20) $$\begin{aligned}\overline{\rho(g)}^T M\rho(g)&=\sum_{i=1}^{t}\overline{\rho(g)}^T\overline{\rho(g_i)}^T\rho(g_i)\rho(g)\\&=\sum_{i=1}^{t}\overline{\rho(g_ig)}^T\rho(g_ig)\\&=\sum_{i=1}^{t}\overline{\rho(g_i)}^T\rho(g_i)\\&=M\end{aligned}$$

となる．ゆえに，Mはすべての $\rho(g), g\in G$ で不変な正定値エルミート形式Hに対応している．変数変換

(16.9.21) $$x_j=\sum_{k=1}^{n} c_{jk}x_k',\quad j=1, \cdots, n$$

により，Hは $\overline{x_1'}x_1'+\cdots+\overline{x_n'}x_n'=I(\bar{x}',x')$ となり，それに対応して，$\rho(g)$ と同値な表現

$$\rho'(g)=C^{-1}\rho(g)C,\quad C=(c_{jk}) \tag{16.9.22}$$

はユニタリ表現となるが，これが証明すべきことだった．

これは行列の形で証明することもできる．

$$\bar{C}^T MC=I,\quad M=\overline{C^{-1T}}IC^{-1} \tag{16.9.23}$$

で，すべての $g\in G$ に対し

$$\overline{\rho(g)}^T M\rho(g)=M \tag{16.9.24}$$

だから，

$$\overline{\rho(g)}^T\overline{C^{-1T}}C^{-1}\rho(g)=\overline{C^{-1T}}C^{-1}, \tag{16.9.25}$$

したがって，

$$\overline{(C^{-1}\rho(g)C)}^T C^{-1}\rho(g)C=I \tag{16.9.26}$$

となり，$\rho'(g)=C^{-1}\rho(g)C$ はユニタリ行列である．

16.10. 群表現のいくつかの例

無限行列群の別の行列群による表現という物理学者にも興味があると思われる例から始めよう．2次元のユニモジュラー[1]ユニタリ行列の全体 U_2 は

$$\begin{pmatrix} \alpha, & \beta \\ -\bar{\beta}, & \bar{\alpha} \end{pmatrix} \qquad \alpha\bar{\alpha}+\beta\bar{\beta}=1 \tag{16.10.1}$$

という形の行列から成っている．ただし，α,β は $\alpha\bar{\alpha}+\beta\bar{\beta}=1$ という条件を満たす任意の複素数である．したがって U_2 というのは

$$\begin{aligned} u&=\alpha u'+\beta v' \\ v&=-\bar{\beta}u'+\bar{\alpha}v' \end{aligned} \qquad \alpha\bar{\alpha}+\beta\bar{\beta}=1 \tag{16.10.2}$$

という線形変換の全体がつくる群で，これらは $\bar{u}u+\bar{v}v$ を不変にする．複素変数 u,v を使って3つの実変数

$$\begin{aligned} x_1&=\bar{u}v+\bar{v}u, \\ x_2&=\frac{1}{i}(\bar{u}v-\bar{v}u), \\ x_3&=\bar{u}u-\bar{v}v \end{aligned} \tag{16.10.3}$$

1）行列式が1という意味

が定義できる．

(16.10.4)
$$x_1^2+x_2^2+x_3^2=(\bar{u}u+\bar{v}v)^2$$

となっていることに注意する．線形変換 (16.10.2) を (16.10.3) に代入すると，x についての実線形変換が得られるが，(16.10.4) により，これは実直交群 O_3 に属することがわかる．(16.10.2) により引き起こされる x についての線形変換は

(16.10.5)
$$x_1=\frac{1}{2}(\alpha^2+\bar{\alpha}^2-\beta^2-\bar{\beta}^2)x_1'+\frac{i}{2}(-\alpha^2+\bar{\alpha}^2-\beta^2-\bar{\beta}^2)x_2'+(-\alpha\beta-\overline{\alpha\beta})x_3',$$
$$x_2=\frac{i}{2}(\alpha^2-\bar{\alpha}^2-\beta^2+\bar{\beta}^2)x_1'+\frac{1}{2}(\alpha^2+\bar{\alpha}^2+\beta^2+\bar{\beta}^2)x_2'+\quad i(\overline{\alpha\beta}-\alpha\beta)x_3',$$
$$x_3=(\alpha\bar{\beta}+\beta\bar{\alpha})x_1'+\qquad i(\alpha\bar{\beta}-\beta\bar{\alpha})x_2'+\qquad (\alpha\bar{\alpha}-\beta\bar{\beta})x_3'$$

となる．したがって (16.10.5) により群 U_2 の実3次元直交群 O_3 における表現 ρ が与えられた．この表現は忠実ではなく，U_2 の元 $\begin{pmatrix}1, 0\\0, 1\end{pmatrix}$ と $\begin{pmatrix}-1, & 0\\ 0, & -1\end{pmatrix}$ が共に O_3 の単位元に表現され，2対1である．U_2 は真回転（行列式が+1）の全体のつくる群で表現されている．真回転から成る群 G の U_2 における逆像は **2重群** (double group) $2G$ として知られている．群 $2G$ は，位数2の部分群の G に同型な商群による拡大群である．

物理系 S に O_3 の部分群 K が付随しているとき，S の電子スピンの波動関数

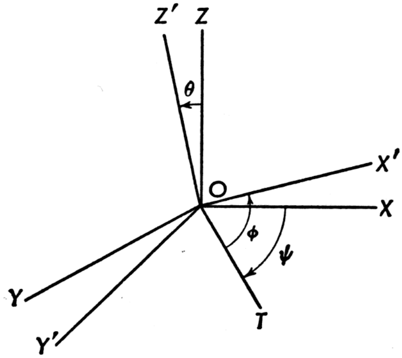


図 7.　3次元の回転

には2重群 $2K$ が付随するということが Pauli [1] により発見された.

U_2 と U_2 の O_3 における表現との間の具体的な関係を与える公式が (16.10.5) 以外にもある. 3次元ユークリッド空間の真回転 (すなわち O_3 の元) が与えられたとき, 座標平面 XOY とその像 $X'OY'$ とが直線 OT で交わっているとする. ϕ を角 $X'OT$, ψ を角 XOT, θ を角 ZOZ' とし (図7参照),

(16.10.6) $$\alpha=\cos\frac{\theta}{2}\exp i\left(\frac{\phi+\psi}{2}\right),\quad \beta=i\sin\frac{\theta}{2}\exp i\left(\frac{\phi-\psi}{2}\right)$$

と置けば, (16.10.1) の対応する U_2 の元が得られる. XOY と $X'OY'$ が一致する (すなわち, Z 軸についての回転) ときにも, $\theta=0$, $\phi=0$, そして Z 軸のまわりの回転角を ψ とすれば上の式は成り立つ.

正4面体の真回転の全体のつくる群は, その4つの頂点上の置換群として忠実に表現される. 各頂点に対し, その頂点を固定する部分群は, 向いの面の3頂点を回転させる位数3の群である. 2つの頂点を固定し, 残りの2つの頂点を取り換えるという対称は, ある平面に関する鏡映で, 向きを逆にするから真回転ではない. したがって4面体群, つまり真回転全体のつくる群は, 位数12で, 4文字の上の交代群 A_4 に同型である. 元を共役類にわけると,

(16.10.7) $$\begin{aligned} C_1&=(1),\\ C_2&=(12)(34),\ (13)(24),\ (14)(23),\\ C_3&=(123),\ (142),\ (134),\ (243),\\ C_4&=(132),\ (124),\ (143),\ (234) \end{aligned}$$

となる. 共役類の積は

(16.10.8) $$\begin{aligned} C_1C_i&=C_iC_1=C_i,\quad i=1,2,3,4,\\ C_2^2&=3C_1+2C_2,\\ C_2C_3&=C_3C_2=3C_3,\\ C_2C_4&=C_4C_2=3C_4,\\ C_3^2&=4C_4,\\ C_3C_4&=C_4C_3=4C_1+4C_2,\\ C_4^2&=4C_3 \end{aligned}$$

となる．

群環の中心Zの巾等元でZの直交基底となるものを探そう．eZ がZの極小イデアルになるような巾等元eはこれらの中にあり，逆も成り立つ．この過程はZの（両側）イデアルの直和への分解とみることもできる．特に任意の真の零因子からZの真イデアルがつくれる．したがって両側イデアルの真零因子をみつければ，もっと小さい両側イデアルがみつかり，結局極小イデアルがみつかる．そしてこれらから直交巾等元がみつかるわけである．一般にfをZの巾等元とする．すべての共役類に対し，$fC_i=a_if$ が成り立てば，fZ はZの極小イデアルで，fは直交巾等元の１つである．ある共役類Cに対し，fC とfが１次独立ならば，fC^j，$j=0, \cdots, s-1$ が１次独立で，fC^s はこれらに従属になるような最小の整数をsとすると，$f(C^s+a_1C^{s-1}+\cdots+a_s)=0$ という関係がある．必要ならば，$x^s+a_1x^{s-1}+\cdots+a_s=0$ の根を係数体につけ加える．uを１つの根とすると，$f(C-u)$ はイデアル fZ における真零因子で，もっと小さい両側イデアルが得られる．４面体群を例にとって，この一般的方法を説明しよう．

位数gの任意の群において，全部の元の和をgで割ったものは巾等元eで，そのイデアルはZにおいて極小である．この巾等元はGの恒等表現に対応する．ここでは $e_1=(C_1+C_2+C_3+C_4)/12$ である．（16.10.8）より

(16.10.9)
$$C_2^2-2C_2-3C_1=(C_2-3C_1)(C_2+C_1)=0$$

という関係があることを注意しておく．したがって C_2-3C_1 と C_2+C_1 は共に零因子である．実際 $(C_2-3C_1)Z$ は極小イデアルで，$e_2=(3C_1-C_2)/4$ という巾等元がこの極小イデアルを生成している．また $e_1e_2=e_2e_1$ となっている．$f=1-e_1-e_2$ という巾等元は，Z の残りの部分の単位元になっているはずである．fZ は２次元のはずで，Zの基底をつくる直交巾等元のうち，残りのものを e_3 と e_4とすると，$f=e_3+e_4$ とならなければならない．そして

(16.10.10)
$$\begin{aligned} f\ &=(2C_1+2C_2-C_3-C_4)/12, \\ fC_1&=f, \\ fC_2&=3f, \end{aligned}$$

$$fC_3=(-4C_1-4C_2+8C_3-4C_2)/12,$$
$$fC_4=(-4C_1-4C_2-4C_3+8C_4)/12,$$

となっていることが分かる.

(16.10.11) $$fC_4+fC_3+4f=0$$

という関係から，イデアル fZ が2次元であることが分かる.

(16.10.12) $$f(C_3{}^2+4C_3+16)=0$$

という関係が成り立つ. そこで有理数体に1の複素3乗根 $\omega=(-1+\sqrt{3}\,i)/2$ を付け加えたものを係数体にすると，(16.10.12) は

(16.10.13) $$f(C_3-4\omega)(C_3-4\omega^2)=0$$

となる. したがって $f(C_3-4\omega)$ および $f(C_3-4\omega^2)$ からつくった主イデアルはイデアル fZ よりも小さい. $f(C_3-4\omega)$ と (16.10.14) における巾等元 e_3, また $f(C_3-4\omega^2)$ と e_4 との違いはスカラー倍だけである.

(16.10.14)
$$\begin{aligned}
&e_1=(C_1+C_2+C_3+C_4)/12,\\
&e_2=(3C_1-C_2)/4,\\
&e_3=(C_1+C_2+\omega C_3+\omega^2C_4)/12,\\
&e_4=(C_1+C_2+\omega^2C_3+\omega C_4)/12,\\
&e_1+e_2+e_3+e_4=C_1=1.
\end{aligned}$$

極小巾等元を共役類によって表わせれば，直ちに指標の表が書き下せ，逆も成り立つ. 定理16.6.10の直前で

(16.10.15) $$C_k=h_k\sum_a\frac{\chi_k{}^a}{n_a}e_a$$

という関係が成り立つことを示した. 両辺に $\overline{\chi_k{}^b}$ を掛けて k について加えれば,

(16.10.16) $$\sum\overline{\chi_k{}^b}C_k=\sum_{a,k}\frac{h_k\overline{\chi_k{}^b}\chi_k{}^ae_a}{n_a}$$

となる. 右辺をまず k について加え,

(16.10.17) $$\sum_k h_k\overline{\chi_k{}^b}\chi_k{}^a=\delta_{ab}g$$

という直交関係を使い，次に a について加えると，$a=b$ 以外の項はすべて0

となるから，(16.10.16) という関係式は

$$\sum_k \overline{\chi_k{}^b} C_k = \frac{g e_b}{n_b} \tag{16.10.18}$$

となる．これは

$$e_b = \frac{n_b}{g} \sum_k \overline{\chi_k{}^b} C_k \tag{16.10.19}$$

という形にも書ける．単位元からなる共役類での指標は次数 $\overline{\chi_1{}^b} = n_b$ であるから，e_b を (16.10.19) のように表わしたときの C_1 の係数は $n_b{}^2/g$ でなければならず，これから n_b が分かり，(16.10.19) を使うと残りの指標も読みとれる．

一般的規則 (16.10.19) と 4 面体群についての表 (16.10.14) を使うと，4 面体群の指標の表が書き下せる．

(16.10.20)

	C_1	C_2	C_3	C_4
ρ_1	1	1	1	1
ρ_2	3	-1	0	0
ρ_3	1	1	ω^2	ω
ρ_4	1	1	ω	ω^2.

逆に，指標の表 (16.10.20) があれば，(16.10.19) を使うことにより，(16.10.14) の極小直交巾等元を書き下すことができる．

ρ_1, ρ_3, ρ_4 という 3 つの 1 次既約表現はもちろん指標の表から直ちに分かる．

4 面体群を A_4 とみたときの表現は，定理 16.6.15 により恒等表現と別の既約表現の和になるが，それは次数が 3 だから ρ_2 でなければならない．変数 x_1, x_2, x_3, x_4 についての A_4 の置換は $x_1+x_2+x_3+x_4$ という線形形式を固定し，$y_1=x_1-x_4$, $y_2=x_2-x_4$, $y_3=x_3-x_4$ で張られる補空間をそれ自身に写す．ただし置換 (12)(34) というのは

$$\begin{aligned} x_1 &= \quad x_2{}', \\ x_2 &= x_1{}', \\ x_3 &= \qquad\quad x_4{}', \\ x_4 &= \qquad x_3{}' \end{aligned} \tag{16.10.21}$$

という線形変換のことで，y については

$$\begin{aligned} y_1 &= \quad\ y_2' - y_3', \\ y_2 &= y_1' \quad\ - y_3', \\ y_3 &= \qquad\quad - y_3' \end{aligned} \tag{16.10.22}$$

となる．ゆえに

$$\rho_2[(12)(34)] = \begin{pmatrix} 0, & 1, & -1 \\ 1, & 0, & -1 \\ 0, & 0, & -1 \end{pmatrix} \tag{16.10.23}$$

となる．同様に

$$\rho_2[(123)] = \begin{pmatrix} 0, & 1, & 0 \\ 0, & 0, & 1 \\ 1, & 0, & 0 \end{pmatrix}$$

となる．2つの元 (12)(34) と (123) で群全体が生成されるから，これで表現が完全に決ったわけである．これは ρ_2 の直交形式ではないが，4面体群は8面体群の部分群だから，次の例から直交形式が得られる．

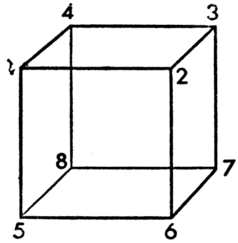


図 8. 立方体の対称

立方体の対称全体のつくる群は第1章例2で論じられた．真回転の全体は位数24の群 G_{24} をつくり，これは

$$a = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 2, 3, 4, 1, 6, 7, 8, 5 \end{pmatrix} = (1234)(5678),$$

$$b = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 1, 4, 8, 5, 2, 3, 7, 6 \end{pmatrix} = (1)(245)(7)(386)$$

で生成される．群 G_{24} は正8面体の対称全体のつくる群でもある．正8面体と

いうのは立方体の各面の中心に頂点を持つように立方体の中に埋め込まれているとみることができる．したがって G_{24} は正8面体の6つの頂点に対応する立方体の6つの面上の置換群としても表現される．8面体の6つの頂点に対応する6つの変数を使うことにする．

変数	立方体の面	8面体の頂点
x_1	1234	$(0, 0, 1)$
x_2	1256	$(0, 1, 0)$
x_3	1458	$(-1, 0, 0)$
x_4	5678	$(0, 0, -1)$
x_5	3478	$(0, -1, 0)$
x_6	2367	$(1, 0, 0)$

すると $a=(x_1)(x_4)(x_2, x_6, x_5, x_3)$, $b=(x_1, x_3, x_2)(x_4, x_6, x_5)$ となる．G_{24} の24個の元は次のようになる．各元を x に関する置換としての形，および x, y, z 座標についての単項線形変換としての形を与えることにする．

共役類	g_i	置　換	$x,\ y,\ z$
C_1	g_1	(x_1)	$x,\ y,\ z$
C_2	g_2	$(x_1)(x_4)(x_2, x_5)(x_3, x_6)$	$-x, -y,\ z$
	g_3	$(x_1, x_4)(x_2)(x_5)(x_3, x_6)$	$-x,\ y, -z$
	g_4	$(x_1, x_4)(x_2, x_5)(x_3)(x_6)$	$x, -y, -z$
C_3	g_5	$(x_1)(x_4)(x_2, x_6, x_5, x_3)$	$-y,\ x,\ z$
	g_6	$(x_1)(x_4)(x_2, x_3, x_5, x_6)$	$y, -x,\ z$
	g_7	$(x_2)(x_5)(x_1, x_3, x_4, x_6)$	$z,\ y, -x$
	g_8	$(x_2)(x_5)(x_1, x_6, x_4, x_3)$	$-z,\ y,\ x$
	g_9	$(x_3)(x_6)(x_1, x_2, x_4, x_5)$	$x, -z,\ y$
	g_{10}	$(x_3)(x_6)(x_1, x_5, x_4, x_2)$	$x,\ z, -y$
C_4	g_{11}	$(x_1, x_2)(x_3, x_6)(x_4, x_5)$	$-x,\ z,\ y$
	g_{12}	$(x_1, x_3)(x_2, x_5)(x_4, x_6)$	$-z, -y, -x$
	g_{13}	$(x_1, x_4)(x_2, x_6)(x_3, x_5)$	$y,\ x, -z$
	g_{14}	$(x_1, x_4)(x_2, x_3)(x_5, x_6)$	$-y, -x, -z$
	g_{15}	$(x_1, x_5)(x_2, x_4)(x_3, x_6)$	$-x, -z, -y$
	g_{16}	$(x_1, x_6)(x_2, x_5)(x_3, x_4)$	$z, -y,\ x$

$$C_5 \begin{cases} g_{17} & (x_1, x_2, x_3)(x_4, x_5, x_6) & -z, -x, \ \ y \\ g_{18} & (x_1, x_2, x_6)(x_3, x_4, x_5) & z, \ \ x, \ \ y \\ g_{19} & (x_1, x_3, x_2)(x_4, x_6, x_5) & -y, \ \ z, -x \\ g_{20} & (x_1, x_3, x_5)(x_2, x_4, x_6) & y, -z, -x \\ g_{21} & (x_1, x_5, x_3)(x_2, x_6, x_4) & -z, \ \ x, -y \\ g_{22} & (x_1, x_5, x_6)(x_2, x_3, x_4) & z, -x, -y \\ g_{23} & (x_1, x_6, x_2)(x_3, x_5, x_4) & y, \ \ z, \ \ x \\ g_{24} & (x_1, x_6, x_5)(x_2, x_4, x_3) & -y, -z, \ \ x \end{cases}$$

G_{24} のこの表現における偶置換の全体（共役類 C_1, C_2, C_5 の元）を $+1$ に，奇置換の全体（共役類 C_3, C_4 の元）を -1 に写すと，これは恒等表現とは異なる1次表現を与える．既約表現の次数 n_i は

(16.10.25) $$n_1^2+n_2^2+n_3^2+n_4^2+n_5^2=24$$

という関係を満たす．$n_1=1$, $n_2=1$ だから，n_3, n_4, n_5 は2，3，3でなければならない．上に与えた3次表現の指標は

(16.10.26) $$\chi_1=3,\ \ \chi_2=\chi(g_2)=-1,\ \ \chi_3=\chi(g_5)=1,$$
$$\chi_4=\chi(g_{11})=-1,\ \ \chi_5=\chi(g_{17})=0$$

である．一般に，表現 ρ を既約表現 ρ_a の和として表わしたとき

(16.10.27) $$\rho=\sum_a c_a\rho_a$$

となったとすると，i 番目の共役類では

(16.10.28) $$\chi_i=\sum_a c_a\chi_i{}^a$$

となり，直交関係により

(16.10.29) $$\sum_i h_i\chi_i\bar{\chi}_i=g\sum_a c_a{}^2$$

となる．上の3次表現については，(16.10.26) により

(16.10.30) $$\sum_i h_i\chi_i\bar{\chi}_i=24$$

となるから，$\sum_a c_a{}^2=1$ で，この表現（ρ_4 と書くことにする）は既約である．ρ_4 は直交表現であって，偶置換の全体（共役類 C_1, C_2, C_5 の元）は4面体群と同型な部分群をつくっているから，これは4面体群について論じたときに約束した3次直交表現を与えている．

これで指標の表の一部分が得られた.

(16.10.31)

	$h_1=1$	$h_2=3$	$h_3=6$	$h_4=6$	$h_5=8$
	C_1	C_2	C_3	C_4	C_5
ρ_1	1	1	1	1	1
ρ_2	1	1	-1	-1	1
ρ_3	2	y_2	y_3	y_4	y_5
ρ_4	3	-1	1	-1	0
ρ_5	3	z_2	z_3	z_4	z_5

第2列とそれ自身および第1列との直交関係により

(16.10.32) $$1+1+2y_2-3+3z_2=0,$$
$$1+1+y_2^2+1+z_2^2=8$$

が得られる. これらの方程式から, $y_2=2$, $z_2=-1$ または $y_2=-22/13$, $z_2=19/13$ となるが, y_2 は1の平方根2つの和であるから, $y_2=\pm1\pm1$ で, $y_2=2$ でなければならず, $z_2=-1$ となる.

第3列と第1列および第2列との直交関係より

(16.10.33) $$1-1+2y_3+3+3z_3=0,$$
$$1-1+2y_3-1-z_3=0$$

が得られ, これらの方程式から $y_3=0$, $z_3=-1$ が得られる. 同様にして残った列の値もみつけることができる. 完全な指標の表は次のようになる.

(16.10.34)

	$h_1=1$	$h_2=3$	$h_3=6$	$h_4=6$	$h_5=8$
	C_1	C_2	C_3	C_4	C_5
ρ_1	1	1	1	1	1
ρ_2	1	1	-1	-1	1
ρ_3	2	2	0	0	-1
ρ_4	3	-1	1	-1	0
ρ_5	3	-1	-1	1	0

立方体の頂点上の置換群とみたときの G_{24} の8次表現 ρ の指標は

(16.10.35)

	C_1	C_2	C_3	C_4	C_5
χ	8	0	0	0	2

である.

(16.10.36)
$$\rho=\sum_a c_a\rho_a,$$
$$\chi_i=\sum_a c_a\chi_i{}^a$$

とすると，直交関係より

(16.10.37)
$$\sum_i h_i\chi_i\overline{\chi_i{}^b}=\sum_{i,a} c_a h_i\chi_i{}^a\overline{\chi_i{}^b}=g\sum_a c_a\delta_{ab}=gc_b$$

となるから，上の指標より各既約表現 ρ_b が ρ に現われる重複度 c_b が求まり，ρ の分解が分かる．このようにして（16.10.35）より

(16.10.38)
$$\rho=\rho_1+\rho_2+\rho_4+\rho_5$$

となることが分かる．これを使うと ρ から ρ_5 を具体的に求めることができる．（16.10.19）と指標の表（16.10.34）を使うと

(16.10.39)
$$e_5=(3C_1-C_2-C_3+C_4)/4$$

となることが分かる．G_{24} の表現 ρ は群環 R_G の表現にもなっており，e_5 の表現は

(16.10.41)
$$\rho(e_5)=\frac{1}{4}\begin{pmatrix} 3, & -1, & -1, & -1, & -1, & -1, & 3, & -1 \\ -1, & 3, & -1, & -1, & -1, & -1, & -1, & 3 \\ -1, & -1, & 3, & -1, & 3, & -1, & -1, & -1 \\ -1, & -1, & -1, & 3, & -1, & 3, & -1, & -1 \\ -1, & -1, & 3, & -1, & 3, & -1, & -1, & -1 \\ -1, & -1, & -1, & 3, & -1, & 3, & -1, & -1 \\ 3, & -1, & -1, & -1, & -1, & -1, & 3, & -1 \\ -1, & 3, & -1, & -1, & -1, & -1, & -1, & 3 \end{pmatrix}$$

となることが分かる．

$x_i=(0,\cdots,\overset{(i)}{1},\cdots,0)$, $i=1,\cdots,8$ を ρ に対する表現加群 M の基底にとると，行列 $\rho(e_5)$ の行は部分加群 Me_5 を張り，その次元は当然3である．最初の3行 r_1, r_2, r_3 を基底にとることもできるが，r_1+r_3, r_1+r_2, r_2+r_3 というベクトルのスカラー倍を基底に取った方が便利である．この基底は

$$
\begin{aligned}
y_1&=x_1-x_2+x_3-x_4+x_5-x_6+x_7-x_8,\\
y_2&=x_1+x_2-x_3-x_4-x_5-x_6+x_7+x_8,\\
y_3&=x_1-x_2-x_3+x_4-x_5+x_6+x_7-x_8
\end{aligned}
\tag{16.10.41}
$$

となる．この基底に関し

$$
\begin{aligned}
\rho_5(a)&=\begin{pmatrix}-1, & 0, & 0\\ 0, & 0, & -1\\ 0, & 1, & 0\end{pmatrix}=\begin{pmatrix}y_1, & y_2, & y_3\\ -y_1, & -y_3, & y_2\end{pmatrix}\\
\rho_5(b)&=\begin{pmatrix}0, & 1, & 0\\ 0, & 0, & 1\\ 1, & 0, & 0\end{pmatrix}=\begin{pmatrix}y_1, & y_2, & y_3\\ y_2, & y_3, & y_1\end{pmatrix}
\end{aligned}
\tag{16.10.42}
$$

となることが分かる． これらにより表現 ρ_5 全体が生成される． したがって (16.10.42) で与えられる ρ_5 は G_{24} の単項かつ直交表現である．しかし $\rho_5(a)$ の行列式が -1 であるから，これは真回転のつくる群ではない．C_3 および C_4 の元に対しては ρ_4 に -1 をかけると，ρ_5 と同値な表現が得られる．したがって ρ_5 は ρ_4 と ρ_2 のクロネッカー積である．

表現 ρ_3 は忠実ではなく，その核は単位元と C_2 の元から成り，位数 4 である．生成元として

$$
\rho_3(a)=\begin{pmatrix}0, & 1\\ 1, & 0\end{pmatrix},\quad \rho_3(b)=\begin{pmatrix}0, & 1\\ -1, & -1\end{pmatrix}
\tag{16.10.43}
$$

がとれる．

G_{24} の真回転群による表現 ρ_4 において

$$
\rho_4(a)=\begin{pmatrix}0, & -1, & 0\\ 1, & 0, & 0\\ 0, & 0, & 1\end{pmatrix},\quad \rho_4(b)=\begin{pmatrix}0, & -1, & 0\\ 0, & 0, & 1\\ -1, & 0, & 0\end{pmatrix}
\tag{16.10.44}
$$

となる．したがって ρ_4 は O_3 の部分群で，U_2 から O_3 の上への写像を与える (16.10.5) を使うと

$$
\frac{\pm 1}{\sqrt{2}}\begin{pmatrix}1-i, & 0\\ 0, & 1+i\end{pmatrix}\to\rho_4(a),\quad \frac{\pm 1}{\sqrt{2}}\begin{pmatrix}1-i, & -1+i\\ 1+i, & 1+i\end{pmatrix}\to\rho_4(b)
\tag{16.10.45}
$$

となることが分かる．2 重群 $D=2G_{24}$ は 8 つの共役類をもつ．一般に 2 重群 $2G$ において，G の共役類 C_i の逆像は $2G$ において C_i の 2 倍の元を持つ 1 つ

の共役類となるか，C_i と同数の元を持つ2つの共役類 C_i' と $C_i''=-C_i'$ になる．

Bethe [1] に従い，Dの元を次の4つの行列

$$1=\begin{pmatrix}1, & 0\\0, & 1\end{pmatrix},\quad \sigma_x=\begin{pmatrix}0, & 1\\1, & 0\end{pmatrix},\quad \sigma_y=\begin{pmatrix}0, & -i\\i, & 0\end{pmatrix},\quad \sigma_z=\begin{pmatrix}1, & 0\\0, & -1\end{pmatrix}$$

を使って表わすことにしよう．Dの元を共役類ごとにまとめると，

$$\begin{aligned}
&E=[1],\\
&R=[-1],\\
&C_2=\pm[-i\sigma_x,\ -i\sigma_y,\ -i\sigma_z],\\
&C_3'=\left[\frac{1\pm i\sigma_x}{\sqrt{2}},\ \frac{1\pm i\sigma_y}{\sqrt{2}},\ \frac{1\pm i\sigma_z}{\sqrt{2}}\right],\\
&C_3''=-C_3',\\
&C_4=\pm\left[\frac{-i(\sigma_y\pm\sigma_z)}{\sqrt{2}},\ \frac{-i(\sigma_z\pm\sigma_x)}{\sqrt{2}},\ \frac{-i(\sigma_x\pm\sigma_y)}{\sqrt{2}}\right],\\
&C_5'=\left[\frac{1}{2}\{1\pm i(\sigma_x+\sigma_y+\sigma_z)\},\ \frac{1}{2}\{1\pm i(-\sigma_x+\sigma_y-\sigma_z)\},\right.\\
&\qquad\left.\frac{1}{2}\{1\pm i(-\sigma_x-\sigma_y+\sigma_z)\},\ \frac{1}{2}\{1\pm i(\sigma_x-\sigma_y-\sigma_z)\}\right],\\
&C_5''=-C_5'
\end{aligned}\tag{16.10.47}$$

となる．

G_{24} はDの準同型像だから，G_{24} の既約表現はDの既約表現でもある．そしてDはさらに3つの既約表現を持っており，それらはDの忠実な表現になっている．それらの指標は

(16.10.48)

	E	R	C_2	C_3'	C_3''	C_4	C_5'	C_5''
ρ_6	2	-2	0	$\sqrt{2}$	$-\sqrt{2}$	0	1	-1
ρ_7	2	-2	0	$-\sqrt{2}$	$\sqrt{2}$	0	1	-1
ρ_8	4	-4	0	0	0	0	-1	1

である．

第17章　自由積と融合積

17.1. 自由積の定義

整列集合 I で添字づけられた群の集合 $G_i(i\in I)$ に対して，その**自由積** $\coprod_i^* G_i$ を次のように定義する．なおこの定義の仕方は，7章での生成元から自由群を作る方法と類似していることに注意しよう．

いま，語

$$a_1a_2\cdots a_t \tag{17.1.1}$$

を考えよう．ここで $a_1a_2\cdots a_t$ は，空集合であるか，または各 $a_i(i=1,\cdots,t)$ がある G_j の元とする．これらの語達の間に，**初等同値**とよばれる関係 $(E1)$, $(E2)$, を次のように定義する．

$(E1)$ a_i がある G_j の単位元であれば，$a_1a_2\cdots a_{i-1}a_ia_{i+1}\cdots a_t$ と $a_1\cdots a_{i-1}a_{i+1}\cdots a_t$ は互いに初等同値である，

$(E2)$ a_i と a_{i+1} が同一の群 G_j に属し，G_j において $a_ia_{i+1}=a_i^*$ であれば，$a_1a_2\cdots a_{i-1}a_ia_{i+1}\cdots a_t$ と $a_1a_2\cdots a_{i-1}a_i^*a_{i+2}\cdots a_t$ は互いに初等同値である．

いま，2つの語 x と y が**同値**であるとは，語の列 $x_1=x$, x_2, x_3, $\cdots$, $x_n=y$ が存在して，各 $i(i=1,\cdots,n-1)$ に対して x_i と x_{i+1} が初等同値であることと定義する．明らかに，ここで定義した同値という関係は，同値関係を満たす．

語 $a_1a_2\cdots a_t$ が**簡約** (reduced) であるとは，（1）どの a_i もそれの属する群 G_j の単位元でなく，かつ（2）各 $i=1,\cdots,t-1$ に対して a_i と a_{i+1} の属する群 G_v 達が相異なることと定義する．

§7.1における と同様に，各語に対してその簡約形を決めるために，W-過程という演算を語 $f=a_1a_2\cdots a_t$ に対して次のように定める．

$W_0=1$.

$W_1=1$ (a_1 がそれの属する群 G_v の単位元のとき).

$$W_1=a_1 \text{（}a_1\text{ がそれの属する群 }G_v\text{ の単位元でないとき）.}$$

次に帰納的に，語 $W_i=b_1b_2\cdots b_s$ が簡約形であるとき，W_{i+1} を次のように定める．

1）$W_{i+1}=b_1\cdots b_sa_{i+1}$（$a_i$ がそれの属する群 G_u の単位元でなく，b_s が G_u に属さないとき）.

2）$W_{i+1}=b_1\cdots b_s$（a_{i+1} がそれの属する群 G_u の単位元のとき）.

3）$W_{i+1}=b_1\cdots b_{s-1}$（$b_s$ と a_{i+1} が同一の群 G_u に属し．G_u において $b_sa_{i+1}=1$ のとき）.

4）$W_{i+1}=b_1\cdots b_{s-1}b_s^*$（$b_s$ と a_{i+1} が同一の群 G_u に属し，G_u において $b_sa_{i+1}=b_s^*\neq 1$ のとき）.

このとき，$W(f)=W_t$ は簡約であり，同値である2つの元に対して W–過程は同じ簡約形を与えることが，§7.1 の場合と同様にして示される．したがって各同値類に属する元に対して一意的に簡約語が定まったわけである．語 $f=a_1a_2\cdots a_t$ が簡約形のとき，t を語 f の**長さ**とよぶ．

語の同値類 $[f_1]$ と $[f_2]$ に対して，その積を

(17.1.2)
$$[f_1][f_2]=[f_1f_2]$$

で定義する．定理 7.1.1 の証明と同様にして，この積が代表系のとり方によらないことが示される．この積は結合的であり，これら同値類の全体は，空語を単位元として，群を作る．この群を G_i 達の自由積とよび，$\overset{*}{\prod_i} G_i$ で表わす．(E1) により，各 G_j の単位元は空語 1 と同値だから，これらの単位元達を区別する必要はない．一方，G_j の単位元と異なる元達は簡約語であり，それらどうしが同一視されることはない．

定理 17.1.1. 群 G が部分群 H_i 達の結び (union) で，各 H_i が群 G_i と同形であるとする．このとき，G は $Q=\overset{*}{\prod_i} G_i$ の準同形像である．

証：定理 7.1.2 における証明と同様に，Q の元 $a_1a_2\cdots a_t$ を考える．いま，a_i が G_j の元で，対応する H_j の元が b_i であるとき，$a_1a_2\cdots a_t$ に対して $b_1b_2\cdots b_t$ を対応させる．このとき，Q において同値な語は，G の同一の元に対応する．ま

た，QからGへのこの対応は積を保つから，これはQから H_i の結び（すなわちG）の上への準同形写像である．

17.2. 融　合　積

整列集合 I で添字づけられた群の集合 $G_i(i\in I)$ を考える．いま，各 G_i がそれぞれ1つの群Uと同型な部分群 U_i を含むと仮定する．ここで，U_i とUの間の同形写像は以下常に固定されていることに注意しよう．そこで，U_i 達をすべて同一視してそれが同一の群 $U^1(\cong U)$ を作るようにして，G_i 達から生成される最も一般の群は何か，という問題を考えよう．この群は，明らかに，自由積 $\prod_i^* G_i$ において $u_i\in U_i$ と $u_j\in U_j$ が上で定めた同形写像によりUの同一の元uに対応するとき u_i と u_j を同一視することにより得られる，$\prod_i^* G_i$ の準同形像である．ところで，そのような群が存在することは明らかであるが，これらの同一視が不可思議な導来関係を引き起こさないという保証はない．たとえば，極端な場合には，$\prod_{i\in I}^* G_i$ のすべての元が単位元と同一視されてしまうかもしれないのである．しかし，以下でみるように，そのようなことは起こらない．実際，この同一視は，どの U_i にも属さない元に対しては何の影響も与えない．

さて，各 U_i をすべて互いに同一視して，G_i 達から生成される群を作ろう．このようにしてできる群を融合積とよぶ．

まず，語 $a_1a_2\cdots a_t$ を考える．ここで各 a_i はそれぞれある G_j の元とする．そこで，初等同値という関係 ($E1$), ($E2$), ($E3$) を次のように定義する．

($E1$) $a_i=1$ であれば，$a_1a_2\cdots a_{i-1}a_ia_{i+1}\cdots a_t$ と $a_1a_2\cdots a_{i-1}a_{i+1}\cdots a_t$ は互いに初等同値である．

($E2$) a_i, a_{i+1} が同一の G_j に属し，G_j において $a_ia_{i+1}=a_i^*$ であれば，$a_1a_2\cdots a_ia_{i+1}\cdots a_t$ と $a_1a_2\cdots a_i^*\cdots a_t$ は互いに初等同値である．

($E3$) $a_i=u_i$ が $U_j\subseteq G_j$ の元で，$b_i=u_k$ が U_k の元で，U_j, U_k とUの間の同形写像により u_i, u_k が同一の元uに対応するとき，$a_1\cdots a_{i-1}a_ia_{i+1}\cdots a_t$ と $a_1\cdots a_{i-1}b_ja_{i+1}\cdots a_t$ は互いに初等同値である．

いま，語xとyが同値であるとは，語の列 $x=x_1$, x_2, …, $x_n=y$ が存在して，すべての $i(i=1,\cdots,n-1)$ に対して x_i と x_{i+1} が初等同値になることと定義する．このようにしてできた同値関係による類 $[f],[g]$ に対して，積を $[fg]$ で定義する．定理 7.1.1 におけるのと同様に，この積は意味を持ち，上の同値類全体はこの乗法に関して群を作る．このようにしてできた群Tを，融合部分群Uを持つG_i達の自由積，あるいは簡単に，G_i達の融合積とよぶ．このようにして群Tの構成はできたが，Tの性質はまだよく分かっているとはいえない．そこで，次に，Tの元に対して，その標準形を定義しよう．

まず，語$f=a_1a_2\cdots a_t$（ここで a_i はある G_j の元）に対してその標準形を定義する．次に，同値な語に対しては，その標準形が等しくなることを示す．したがってTの任意の元に対して標準形が定義されるわけである．

各 $G_i(i\in I)$ に対して，U_i による左剰余類の代表系 x_{ik} を選ぶ．したがって，

(17.2.1)
$$G_i=U_i+U_ix_{i2}+\cdots+U_ix_{in_i},\quad i\in I$$

と表わされる．初等同値の条件（$E1$）により，空語はTの単位元であり，また各G_iの単位元である．また（$E3$）により，すべての $U_i(i\in I)$ がUと同一視されているとみなすことができる．したがって (17.2.1) を書き直せば，

(17.2.2)
$$G_i=U+Ux_{i2}+\cdots+Ux_{in_i},\quad i\in I$$

と表わされる．したがって，元 $g_i\in G_i$ は，

(17.2.3)
$$g_i=u \text{ または } g_i=uz,\quad u\in U,\quad z=x_{ik}\neq 1$$

と表わされる．いま融合積においては語の長さを定義するのに，通常の定義を修正して次のようにすると都合がよい．すなわち，$a_0\in U$のとき$l(a_0a_1\cdots a_t)=t$. $a_1\notin U$ のとき $l(a_1\cdots a_t)=t$ と定義する．すなわち，最初の項がUの元であれば，それを数えないのである．

さて，Tの元fが標準形であるとは，

(17.2.4)
$$f=uz_1z_2\cdots z_t$$

と表わされることと定義する．ここで，$u\in U$, $z_j(j=1,\cdots,t)$ は (17.2.2) で与えられた剰余類の代表系 $x_{ik}\neq 1$ のいずれかで，各 $j=1,\cdots,n-1$ に対して

z_j と z_{j+1} の属する群 G_v 達は相異なるとする．

定理 17.2.1. 融合部分群 U を持つ G_i 達の自由積において，語の各同値類に対して一意的に標準形 $f=uz_1z_2\cdots z_t$ が定まる．ここで $u\in U$ であり，$z_i(i=1,\cdots,t)$ は G_i の U による左剰余類の固定した代表系 $x_{ik}\neq 1$ のいずれかであり，各 $i=1,\cdots,t-1$ に対して z_i と z_{i+1} の属する群 G_v 達は相異なる．

この定理の証明は，7章における補題7.1.1の証明をまねればよい．紙面の都合もあり，この証明は略すことにする．これらのことについてのさらに進んだ研究については，H. Neumann [1, 2] を参照していただきたい．

17.3. Kurosch の定理

この節では，自由積の部分群は自由積であるという Kurosch*) により見い出された定理を証明する．一方，融合積の部分群は必ずしも融合積であるとは限らず，融合積の部分群についての研究は今後に残された問題である．

定理17.3.1. (**Kurosch の定理**). 自由積 $G=\prod_v^* A_v$ の部分群 $H\neq 1$ はそれ自身自由積であり，

$$H=F*\prod_j^* x_j^{-1}U_jx_j$$

と表わされる．ここで F はある自由群，各 $x_j^{-1}U_jx_j$ は G のある自由因子 A_v のある部分群 U_j の共役を表わす．

証：G の自由因子 A_v 達に属する元達の間に整列順序を入れる．すなわち，まず単位元を先頭にし，次に自由因子達の間に整列順序を定め，その次にそれぞれの自由因子の元達 ($\neq 1$) の間に整列順序を定める．次に，これを利用して群 G の元達の間に，字引式順序を入れることを考える．いま，

$$g=a_1a_2\cdots a_t$$

を元 $g\in G$ の簡約形とする．いい変えれば，$g=1$ ならば右辺は空集合であ

*) A. Kurosch [1]. ここで与えられる証明は M. Hall Jr. [6] による。

り，$g \neq 1$ に対しては任意の $i(i=1, \cdots, t-1)$ に対して，$a_i \neq 1$ かつ $a_i a_{i+1}$ が同一の自由因子に属さないとする．このとき，元 g の長さ $l(g)$ を，$g=1$ に対しては $l(g)=0$，$g \neq 1$ に対しては g の簡約形における項 a_i の個数 t と定義する．そこで，Gの元達の間に，字引式順序を次の 1)，2) に従って定義する．

1)　g の長さ：$l(g_1) \neq l(g_2)$，$l(g_1) < l(g_2)$ ならば $g_1 < g_2$.

2)　簡約形 $g=a_1 a_2 \cdots a_t$ の先頭項 a_1 の順序，次に a_2 の順序，…，a_t の順序：$l(g_1)=l(g_2)=t$，$g_1=a_1 a_2 \cdots a_t$，$g_2=b_1 b_2 \cdots b_t$ のときは，$a_1=b_1$，$a_2=b_2$，…，$a_{i-1}=b_{i-1}$ かつ $a_i < b_i$（先に定めた自由因子に属する元達の間の順序に関して）ならば $g_1 < g_2$.

次に，Gの元達の間に，半字引式順序とよばれるもう1つの順序を定義しよう．いま，元 $g \in G$ の長さ $l(g)=t$ が偶数（$=2r$）であるとき，$g=\alpha\beta^{-1}$，$l(\alpha)=l(\beta)=r$，と表わす．また，$l(g)=t$ が奇数（$=2s+1$）であるとき，$g=\alpha a_{s+1}\beta^{-1}$，ここで $l(\alpha)=l(\beta)=s$，と表わす．このとき，G の元達の間に，半字引式順序$\ll$を次の 1)，2)，3)，4) の順番に従って定義する．

1)　g の長さ.

2)　α の字引式順序.

3)　β の字引式順序.

4)　a_{s+1} の順序（$l(g)$ が奇数のときのみ).

さて，G の部分群Hが自由積であることの証明は，次の条件（イ）（ロ）を満たすHの部分集合Kが存在することを，半字引式順序の言葉を用いて示すことによって完成される．

イ）KはHを生成する．

ロ）Kは自由積

$$F * \prod_j^{*} x_j^{-1} U_j x_j \tag{17.3.1}$$

を生成する．ここでFはある自由群，U_j はある自由因子 A_v の部分群とする．

さて，集合 K を次の性質（1），（2）を満たす元 k 達の全体として定義する．すなわち，（1）k は $k \neq 1$ で $k \in H$，（2）k は，半字引式順序が k より

前であるHの元全体から生成される部分群に含まれない.

いま, $H\neq 1$ だから, 単位元と異なるHの元で半字引式順序が最初の元はKに属する. したがってKは空集合でない. 次に, 集合Kから生成された部分群 $<K>$ について考えよう. $<K>\subseteq H$ は明らかである. もし, $<K>\neq H$ であれば, $h\notin <K>$ なる H の半字引式順序が最初の元 h が存在する. このとき, h は半字引式順序に関して h よりも前の元 $h_i\in H$ 達により生成される. ところが h_i 達はすべて $<K>$ に属するから, それらから生成される h も $<K>$ に属し, h のとり方と矛盾する. したがって $<K>=H$ が示された.

さて, Gの元 $u\neq 1$ を $u=\alpha\beta^{-1}$ または $u=\alpha a\beta^{-1}$ と表わす. u の長さが偶数の場合, $u\neq 1$ だから $\beta=\alpha$ ではありえない. 一方 u の長さが奇数の場合には, $\beta=\alpha$ であってもかまわない. いま α を1つ固定し, a をある1つの A_v の元全体を動かすとき, $\alpha a\alpha^{-1}$ と表わされるHの元全体は(単位元とあわせて) A_v のある部分群Bと共役な群 $\alpha B\alpha^{-1}$ を作る. 元 $\alpha a\alpha^{-1}$ を a の**変換**(transform) とよぶことにする.

次に, Kを含む次のような集合 T を考える. すなわち, α と A_v をそれぞれ1つ固定したとき, K に属する変換 $\alpha a\alpha^{-1}(a\in A_v)$ 達から生成される変換 $\alpha a_1\alpha^{-1}(a_1\in A_v)$ の作る集合とKとの合併集合をTと置く.

Hの元 h は,

(17.3.2) $$h=u_1u_2\cdots u_t.$$

ここで $u_i\in T$ または $u_i\in T^{-1}$ (Tに属する元の逆元の集合) と表わされる. さらにこのとき, これらの u_i 達を, (a) $u_iu_{i+1}\neq 1(i=1,\cdots,t-1)$, かつ (b) ひきつづいた2元 u_i, u_{i+1} は同じ共役群 $\alpha B\alpha^{-1}(B\subseteq A_v)$ に属さない, とすることができる. これらの条件 (a), (b) が満たされているとき, $u_1\cdots u_t$ は半簡約形であるということにする.

さて, この定理を示すためには, 空でない任意の半簡約形が単位元でないことを証明すればよい. もしそのことが証明されれば, Kの変換でない元全体は自由群Fを生成し, さらにHがFと共役群 $\alpha B\alpha^{-1}(B\subseteq A_v)$ 達の自由積であることが示される.

もしuがKの元で$u^{-1}\neq u$であれば，$u\ll u^{-1}$である．なぜならば，$u=(u^{-1})^{-1}$であり，u^{-1}はuより（半字引式順序に関して）前にないからである．また，もし$u, v(u\neq v)$がKの２元であれば，$w=u^{\epsilon}v^{\eta}(\epsilon, \eta=\pm 1)$は$u, v$より後にある．なぜならば，$u, v, w$のうちのどの２つも残りを生成し，$K$の作り方から，$u, v$のいずれも前にある元達からは生成されないからである．これら２つの原理は，TとT^{-1}に属する元達がいつ結びつくかを調べる際の主要な道具である．

Gにおいて積$a_1a_2\cdots a_m$（ここで各a_iは自由因子達のいずれかに属する）を簡約な語に変形していく際に，a_i, a_{i+1}が同一の自由因子A_vに属し$a_ia_{i+1}=a^1$であるときa_iとa_{i+1}がa^1に融合するといい，$a_ia_{i+1}=1$のときa_iとa_{i+1}は削除されるということにする．

補題 17.3.1. もし，$u=\alpha\beta^{-1}\in T$または$u=\alpha a\beta^{-1}\in T$，かつ$\beta\neq\alpha$であれば，$\alpha<\beta$である．

証：$\beta\neq\alpha$だから，$u\in K$である．もし$\beta<\alpha$であれば$u^{-1}\ll u$である．補題証終．

したがって，Tの元uは次の（１），（２），（３）のいずれかでなければならない．

1）$l(u)$は偶数，$u=\alpha\beta^{-1}$，$\alpha<\beta$，$u\in K$.

2）$l(u)$は奇数，$u=\alpha a\beta^{-1}$，$\alpha<\beta$，$u\in K$.

3）$l(u)$は奇数，$u=\alpha a\alpha^{-1}$，uはKに含まれる同種の（すなわち，αとA_vが同じ）変換により生成される．

補題 17.3.2. Tの２元$u, v(u\neq v)$が共に同一の共役群$\alpha B\alpha^{-1}$には属さないとする．また，wを$u^{\epsilon}v^{\eta}$または$v^{\eta}u^{\epsilon}(\epsilon, \eta=\pm 1)$のいずれかとする．このとき，半字引式順序に関して，wはu, vの後にある．このことから，積wにおける融合，削除の仕方に次のような制限がつく．

1）$u=\alpha\beta^{-1}$のとき，β^{-1}が削除されず，αが削除されるならば，β^{-1}の隣り

合った項は融合しない.

2)　$u=\alpha a\beta^{-1}(\alpha<\beta)$ のとき，α と a が削除されず，β^{-1} が削除されるならば，a は融合しない.

3)　$u=\alpha a\alpha^{-1}\in\alpha B\alpha^{-1}$ のとき，α と a が削除されず，$v^{\eta}=\alpha a^{1}\sigma(a, a^{1}\in A_{v})$ であれば，元 a^{1} は剰余類 Ba^{1} のうちで最も前にある.

証：$u\neq v$ だから，$u\ll v$ と仮定してよい．もし w が u および v の後になければ，$w\ll v$ である．なぜならば，もし $w=v$ ならば $u=1$（この場合は除いて考えてよい）または $u=v^{2}$ または $u=v^{-2}$ である．ところで，v が変換ならば，v の平方は 1 または同種の変換である．一方，v が変換でなければ，$l(v^{2})>l(v)$ である．したがっていずれの場合も $u=v^{2}$，$u=v^{-2}$ は起こり得ない．したがって $w\ll v$ である.

ところで，u, v, w のいずれの 2 つも残りを生成するから，もし $v\in K$ であれば，w は u, v の後になければならない．したがって v が変換 $v=\alpha a\alpha^{-1}\in\alpha B\alpha^{-1}$ である場合だけを考えればよい．いま，$u\ll v$ で，$u\notin\alpha B\alpha^{-1}$ だから，$\alpha B\alpha^{-1}$ に属する任意の変換 v^{*} に対して $u\ll v^{*}$ が成り立つ．したがって，もし u と $v=\alpha a\alpha^{-1}$ の間の削除に α（または α^{-1}）のみが表われるならば，u と $v^{*}=\alpha a^{*}\alpha^{-1}\in K$ の間の削除に関してもそうである．このとき，$w^{*}=u^{\epsilon}v^{*}$ または $w^{*}=v^{*}u^{\epsilon}$ が生じ，$w^{*}\ll v^{*}$ でなければならないから $v^{*}\in K$ に矛盾する．したがって，u と $v=\alpha a\alpha^{-1}$ の間の削除には，すべての α および中央項 a の融合，削除が含まれる．したがって $u^{\epsilon}=\sigma a''^{-1}a^{-1}$ である．ここで a'' と a は融合するかまたは削除される．いま，$u\ll v=\alpha a\alpha^{-1}$ だから，$l(\sigma)<l(\alpha)$ または $l(\sigma)=l(\alpha)$ が成り立つ．ここで $u=\sigma a''^{-1}\alpha^{-1}(\sigma<\alpha)$ である．いずれの場合も，u と $\sigma(a''^{-1}a^{*}a'')\sigma^{-1}$ は $av^{*}=\alpha a^{*}\alpha^{-1}(\in K)$ に先行し，しかもそれを生成する．これは矛盾である．したがってもし $w\ll v$ と仮定すれば，いずれの場合にも矛盾が起こる．よって w の順番は u, v の後にある.

そこで，8 つの積 $u^{\epsilon}v^{\eta}$, $v^{\eta}u^{\epsilon}$ 達がいずれも u, v の後にあるということから，

wにおける削除と融合について，この補題で主張しているいくつかの制限がつくことがわかる．これらのことから直ちにわかるように，uまたはvいずれかの半分よりも多くが削除されることはない．また，u, vの片方との融合または削除が他方の先頭（または最後）を別の長さの語と置き換える場合には，そのようにしてできた元は順番が後になる．

補題 17.3.3. 積 $u_1u_2\cdots u_t$ において，$u_i\in T\cup T^{-1}(i=1,\cdots,t)$，$u_iu_{i+1}\neq 1$ $(i=1,\cdots,t-1)$，u_i, u_{i+1} が同一の群 $\alpha B\alpha^{-1}(B\subseteq A_v)$ に含まれないならば，$u_1u_2\cdots u_t$ の簡約形の最後部は次のいずれかの形をしている．

1） β^{-1}，$u_t=\alpha\beta^{-1}$ のとき，

2） $b^*\alpha^{-1}$，$u_t=(\alpha\beta^{-1})^{-1}$ のとき，

3） $\alpha^*\beta^{-1}$，$u_t=\alpha a\beta^{-1}(\alpha<\beta)$ のとき，

4） $a^{-1}\alpha^{-1}$，$u_t=(\alpha a\beta^{-1})^{-1}(\alpha<\beta)$ のとき，

5） $a^*\alpha^{-1}$，$u_t=\alpha a\alpha^{-1}$ のとき

ここで，（2）における b^* および（5）における a^* は，u_t における直前の元，または u_{t-1} の元と融合してできた元のいずれかである．また，（3）における a^* は，u_{t-1} および u_{t-2} の元と融合してできることもある．

証： tに関する帰納法で証明する．$t=1$ のときは自明である．$t=2$ のときは，補題17.3.2と，u^2（ここでは$u=\alpha\beta^{-1}$ または $\alpha a\beta^{-1}$ とする）における削除融合には α, β は関係しないということとから明らかである．次に，t の場合を仮定して，$t+1$ の場合を帰納法を用いて証明しよう．いま，補題17.3.2を上の5つの各々の場合に適用する．また，u_{t+1} に対する5つのそれぞれの場合に，補題 17.3.2 を適用する．この際，補題 17.3.2 から直接には導かれない次の性質を用いる．すなわち，いま，$u_t=\alpha a\alpha^{-1}$ で，α が削除され，かつaが$u_{t-1}=\sigma a'^{-1}\alpha^{-1}$，または同様に $u_{t+1}=\alpha a''\lambda$ と融合するかもしれない．さて，補題 17.3.2 により，a' および a'' はそれぞれ剰余類，Ba', Ba'' における先頭の元である．そこで，もし $a'^{-1}aa''=1$ であれば，a' と a'' は同一の剰余類に属し，したがって $a'=a''$ である．したがって $a=1$, $u_t=1$ となり仮定に反す

る．よって，$a'^{-1}aa''\neq 1$ であり，$u_{t-1}u_tu_{t+1}$ の簡約形は $\sigma(a'^{-1}aa'')\lambda$ である．半簡約形である積 $u_1u_2\cdots u_m$ において，連続した3つの項にわたって融合する場合はこの場合だけである．補題証終．

いま，半簡約形 $h=u_1u_2\cdots u_t$ を簡約形に直すとき，$h\neq 1$ であることが示された．したがって，H は $\alpha\beta^{-1}$ または $\alpha a^{-1}\beta^{-1}(\alpha<\beta)$ を生成元とする無限巡回群達と，自由因子 A_v の部分群 B の共役 $\alpha B\alpha^{-1}$ 達の自由積である．

第18章　Burnside 問題[1)]

18.1. 問題点について

“不連続群論において未決定なことの1つに，すべての元の位数が有限であるような群の位数が有限でなくてもよいかという問題がある”と 1902 年に Burnside [1] は書いている．もちろんここでいっているのは有限生成群のことである．この問題はまだ決定されておらず，このように一般的な形では手をつけられていない．与えられた群は有限生成で，元の位数が有界であるというもっと特殊な形の問題を考える．

Gがr個の元で生成され，Gの元の位数の最小公倍数をnとすると，Gは有限群になるか？　ということが問題になる．これは Burnside 問題として知られている．$x_1, \cdots, x_r$ が群 $B(n, r)$ を生成し，すべての $g \in B(n, r)$ に対し $g^n = 1$ という関係式で定義されているとき，この群は **r 個の生成元をもった位数 n の Burnside 群**とよばれる．r 個の元で生成され，各元の位数がnの約数になっている群は，明らかにこの特別な群の準同型像になる．したがって，Burnside 問題は，$B(n, r)$ の中で有限群になるのはどれか？　という問題に帰着される．

$x_1, \cdots, x_r$ で生成される自由群を F_r，すべての $z^n, z \in F_r$ で生成される全不変部分群をNとすると，$B(n, r) = F_r/N$ である．

18.2. $n=2$ と $n=3$ に対する Burnside 問題

群Gの単位元以外のすべての元の位数が2ならば，$x^2=1$，$y^2=1$，$(xy)^2=1$ より $xyxy=1$，$xy=y^{-1}x^{-1}=yx$ となり，Gは可換群である．したがって x_1,

---

1) 「現代の数学Ⅱ」（岩波）第2章（58頁～129頁）参照

$\cdots, x_r$ で生成され，各元の 2 乗がすべて単位元になるという Burnside 群 $B(2,r)$ は，$x_1, \cdots, x_r$ を基底とする位数 2^r の可換群である．これで $n=2$ の場合は片付いた．

$n=3$ のとき $B(3,r)$ が有限群になることは容易に示される．$B_h=B(3,h)$ が位数 $3^{m(h)}$ だったとする．$(xy)^3=1$ から導かれる

$$yxy=x^{-1}y^{-1}x^{-1} \tag{18.2.1}$$

という関係を使うことにする．B_{h+1} は B_h に新しい生成元 z を付け加えることにより得られる．よって B_{h+1} の元は

$$g=u_1z^{\pm1}u_2z^{\pm1}\cdots z^{\pm1}u_n,\quad u_i\in B_h \tag{18.2.2}$$

という形をしている．g はたかだか 2 つの z を使って表わせることを示そう．(18.2.2) において，同じ指数の項が続けてあったとすると，(18.2.1) を使って $zu_iz=u_i^{-1}z^{-1}u_i^{-1}$ または $z^{-1}u_jz^{-1}=u_j^{-1}zu_j^{-1}$ と直せるから，z の数を 1 つ減らすことができる．したがって g は (18.2.2) の形で，z の指数が交代符号をもつように表わせる．このときもし g が z の項を 3 つ以上もてば，$g=u_1zu_2z^{-1}u_3z\cdots$ において，$g=u_1zu_2z\cdot zu_3z\cdots=u_1u_2^{-1}z^{-1}u_2^{-1}u_3^{-1}z^{-1}u_3^{-1}\cdots$ と z の数を 1 つ減らすことができる．$g=u_1z^{-1}u_2zu_3z^{-1}\cdots$ の場合も同様のことが成り立つから，結局，g はたかだか 2 つの z を使って表わされる．$u_1z^{-1}u_2zu_3=u_1z^{-1}u_2z^{-1}z^{-1}u_3=u_1u_2^{-1}zu_2^{-1}z^{-1}u_3$ とも書けるから，B_{h+1} の任意の元は次の 4 つのうちのどれかの形にすることができる：

$$\begin{aligned}&u_1,\\&u_1zu_2,\\&u_1z^{-1}u_2,\\&u_1zu_2z^{-1}u_3.\end{aligned} \tag{18.2.3}$$

ゆえに B_{h+1} はたかだか $3^m+2\cdot3^{2m}+3^{3m}<3^{3m+1}$ 個の元しかもたず，$m(h+1)\leq 3m(h)$ となる．したがって一般に $m(r)\leq 3^{r-1}$ となり，$B(3,r)$ の位数はたかだか $3^{3^{r-1}}$ である．Burnside の原論文では，もう少し複雑な方法を使って，$m(r)\leq 2^r-1$ というもう少し精密な評価を得ている．ここでは Levi と

van der Waerden [1] により得られた $m(r)=\binom{r}{3}+\binom{r}{2}+r$ という正確な結果を得ることにしよう．

(18.2.1) を3回適用すると，

$$x^{-1}yxzx^{-1}=(x^{-1}yx^{-1})(x^{-1}zx^{-1})$$

(18.2.4) $$=y^{-1}(xy^{-1}z^{-1}x)z^{-1}$$

$$=y^{-1}zyx^{-1}zyz^{-1}$$

という公式が得られる．(18.2.4) において $z=y$ と置くと，$x^{-1}yxyx^{-1}=yx^{-1}y$ となり，

(18.2.5) $$(x^{-1}yx)y=y(x^{-1}yx)$$

となることが分かる．したがって任意の元 y はその任意の共役 $x^{-1}yx$ と可換になる．ゆえに y は $y^{-1}x^{-1}yx$ とも可換となり，交換子を使えば

(18.2.6) $$(y, x, y)=1$$

と書ける．さらにこれから

(18.2.7) $$(x, y)^{-1}=(x^{-1}y^{-1}xy)^{-1}=y^{-1}x^{-1}yx$$

$$=x^{-1}yxy^{-1}=(x, y^{-1})$$

も導かれる．これらより

(18.2.8) $$(x^{-1}, y)=(y, x^{-1})^{-1}=(y, x)=(x, y)^{-1},$$

$$(y, x, x)=((x, y)^{-1}, x)=(x, y, x)^{-1}=1$$

が得られる．次に $(a, c, b)^{-1}=b^{-1}(c^{-1}a^{-1}caba^{-1}c^{-1})ac$ を考えることにし，$x=c$, $y=a^{-1}$, $z=aba^{-1}$ と置いて，(18.2.4) を括弧の中に適用すると，

$$(a, c, b)^{-1}=b^{-1}(aaba^{-1}a^{-1}c^{-1}aba^{-1}a^{-1}ab^{-1}a^{-1})ac$$

$$=b^{-1}a^{-1}bac^{-1}aba^{-1}b^{-1}c$$

$$=(a, b, c)$$

が得られる．また $(a, c, b)^{-1}=((a, c)^{-1}, b)=(c, a, b)$ であるから，これらを合わせると，

(18.2.9) $$(a, b, c)=(c, a, b)=(b, c, a),$$

$$(a, c, b)^{-1}=(a, b, c)$$

が得られた．

次に重さが4の交換子はすべて単位元となることを示そう．まず，複合交換子 $(a,b;c,d)$ を考えよう．(18.2.9) を使うと，

$$
\begin{aligned}
(a,b;(c,d))&=((c,d),a,b)=((c,d,a),b)=(a,c,d,b)\\
&=(a,c,b,d)^{-1}=((a,b,c)^{-1},d)^{-1}\\
&=(a,b,c,d)
\end{aligned}
$$

となる．一方，$(c,d;a,b)=((a,b),c,d)=(a,b,c,d)$ であるから，$(a,b;c,d)=(c,d;a,b)=(a,b;c,d)^{-1}$ となり，

$$(a,b;c,d)=(a,b,c,d)=1 \tag{18.2.10}$$

となる．

前の結果から，重さ3の交換子において同じ元を繰り返して含めば単位元となる．3つの相異なる生成元をもつとき，重さ3の交換子は (18.2.9) により $(x_i,x_j,x_k), i<j<k$, またはこの形の逆元にできる．(18.2.10) により重さ3の交換子は中心にはいり，交換子群は可換群である．ゆえに $B(3,r)$ の任意の元は次の形に書ける．

$$g=x_1{}^{a_1}\cdots x_r{}^{a_r}(x_1,x_2)^{b_{12}}\cdots(x_i,x_j)^{b_{ij}}\cdots(x_i,x_j,x_k)^{c_{ijk}} \tag{18.2.11}$$

ただし，(x_i,x_j) は $i<j$ なるもの，(x_i,x_j,x_k) は $i<j<k$ なるものだけで，指数は0，1，2のいずれかである．このような表わし方の総数は $3^{m(r)}$ である．ただし $m(r)=r+\binom{r}{2}+\binom{r}{3}$ は r 個の生成元 $x_1,\cdots,x_r$ の中から1，2または3個の元をとり出す選び方の数である．ゆえに Burnside 群 $B(3,r)$ の位数は高々 $3^{m(r)}$ で，(18.2.11) の元で指数の中に0でないものがあれば単位元にならないということがいえれば，これが本当の位数である．なぜなら，異なる表現 g_1 と g_2 が $B(3,r)$ の同じ元を表わすとすると，$B(3,r)$ の任意の準同型像でもそうであり，特に位数 3^r の基本可換群でも同じ元を表わす．ゆえに指数 $a_i, i=1,\cdots,r$ は一致する．交換子群は可換だから $g=g_1g_2{}^{-1}=1$ は単位元を表わしているが，b_{ij} または c_{ijk} の中に3を法として0でないものがある．$g=1$ を $B(3,r)$ の1つの関係とみなすと，これは $x_s=1,\ s\neq i,j,k$ という関係を付け加えても成り立つ．ゆえに $B(3,r)$ の位数が $3^{m(r)}$ であることを示

すためには，$B(3,3)$ の位数がちょうど 3^7 であることを示せばよい．

$B(3,3)$ を位数 3^7 の群として構成するために，定理 6.5.1 と定理 6.5.2 で与えられた半直積を使うことにする．

(18.2.12)
$$C_1=x,\ C_2=y,\ C_3=z,\ C_4=(x,y),$$
$$C_5=(x,z),\ C_6=(y,z),\ C_7=(x,y,z)$$

と書くことにする．まず，$A=\{C_4,C_5,C_6,C_7\}$ をつくると，これは位数 3^4 の基本可換群である．次に，Aに

(18.2.13)
$$C_3{}^3=1,\ C_3{}^{-1}C_4C_3=C_4C_7,\ C_3{}^{-1}C_5C_3=C_5,$$
$$C_3{}^{-1}C_6C_3=C_6,\ C_3{}^{-1}C_7C_3=C_7$$

という関係により C_3 をつけ加えて拡大する．(18.2.13) という関係により，C_3 による変換が A の位数 3 の自己同型を引き起こすことをいえば，定理 6.5.1 と 6.5.2 により，群 $B=\{A,C_3\}$ は位数 3^5 で巡回群 C_3 による A の拡大になる．同様に

(18.2.14)
$$C_2{}^3=1,\ C_2{}^{-1}C_3C_2=C_3C_6{}^{-1},\ C_2{}^{-1}C_4C_2=C_4,$$
$$C_2{}^{-1}C_5C_2=C_5C_7{}^{-1},\ C_2{}^{-1}C_6C_2=C_6,\ C_2{}^{-1}C_7C_2=C_7$$

という関係を使うと，Bを C_2 により拡大して位数 3^6 の $H=\{B,C_2\}$ が得られることが分かる．最後に

(18.2.15)
$$C_1{}^3=1,\ C_1{}^{-1}C_2C_1=C_2C_4{}^{-1},\ C_1{}^{-1}C_3C_1=C_3C_5{}^{-1},$$
$$C_1{}^{-1}C_4C_1=C_4,\ C_1{}^{-1}C_5C_1=C_5,\ C_1{}^{-1}C_6C_1=C_6C_7,$$
$$C_1{}^{-1}C_7C_1=C_7$$

を使うと，位数 3^7 の群 $G=\{C_1,H\}$ がHを C_1 により拡大することにより得られる．これらの関係からGの級は 3 で，集中公式

(18.2.16)
$$(PQ)^3=P^3Q^3(Q,P)^3(Q,P,P)(Q,P,Q)^5$$

が成り立つ．$P=z$，Q はA の任意の元と置くと，B は指数が 3 であることが分かる．同様にして H と G も指数が 3 であることが順番に示される．したがって $G=B(3,3)$ の位数は 3^7 で，これから一般の場合の定理が導かれることはすでにみた通りである．

定理 18.2.1. Burnside 群 $B(3,r)$ の位数は $3^{m(r)}$ である．ただし $m(r)=r+\binom{r}{2}+\binom{r}{3}$ で，$B(3,r)$ の元は (18.2.11) の形に一意的に表わされる．

18.3. $B(4,r)$ の有限性

Burnside の原論文において，$B(4,2)$ の位数は高々 2^{12} であることが示された．Sanov [1] により $B(4,r)$ はすべての r について有限群であることが証明された．$B(4,r)$ の正確な位数は知られていないが，$B(4,2)$ の位数は実際に 2^{12} である．

定理 18.3.1. $B(4,r)$ は有限群である．

証：Hをその元の位数がすべて4を割るような有限群とする．Hに位数4の元bをつけ加えて拡大した群$G=H\cup(b)$ において，すべての元の4乗が単位元になるとすれば，Gは有限群になるということを示したい．これは，まずHにb^2をつけ加えて群 $H_1=H\cup(b^2)$ をつくり，次にH_1にbを付け加えて$G=H_1\cup(b)=H\cup(b)$ をつくるという2段階に分けて行なうことができる．これらの拡大はいずれも前の群にその平方がはいっている元を付け加えている．したがって，有限群Hに $x^2\in H$ となる元xを付け加え，$z\in H\cup(x)$ ならば $z^4=1$ となるとすると $H\cup(x)$ は有限群になるということを示せばよい．

$x^2\in H$ ならば，$H\cup(x)$ の任意の元 g は

(18.3.1) $$g=h_1xh_2xh_3x\cdots h_{n-1}xh_n,\quad h_i\in H$$

という形をしている．$(xh)^4=1$ という関係より

(18.3.2) $$xhx=h^{-1}x^{-1}h^{-1}x^{-1}h^{-1}=h^{-1}x(x^2h^{-1}x^2)xh^{-1}$$
$$=h^{-1}xh^*xh^{-1}$$

を得る．ここで h^* もHの元である．したがって (18.3.2) を使って (18.3.1) の語の長さnを増すことなしに，

(18.3.3) $$h_1xh_2\cdots xh_{i-1}h_i{}^{-1}xh_i{}^*xh_i{}^{-1}h_{i+1}x\cdots xh_n$$

という形に変えることができる．もし (18.3.1) においてある h_j, $2\leq j\leq n-1$

が1ならば，$x^2=h\in H$ と置くことにより，長さを減らすことができる．また(18.3.2) を何回か使うことにより，いくつかの h_j を1に変えることができる．

Sanov は (18.3.2) を繰り返し使うことにより h_{i-1} を $h_{i-1}h_i^{-1}$ に，h_{i-2} を $h_{i-2}(h_{i-1}h_i^{-1})^{-1}=h_{i-2}h_ih_{i-1}^{-1}, \cdots$ と置き換えられるということに気がついた．このようにして h_2 は $h_2, h_2h_3^{-1}, h_2h_4h_3^{-1}, h_2h_4h_5^{-1}h_3^{-1}, \cdots, h_2h_4\cdots h_{2s}h_{2s-1}^{-1}\cdots h_3^{-1}, h_2h_4\cdots h_{2s}h_{2s+1}^{-1}\cdots h_3^{-1}$ のどの1つにでも置き換えることができる．もしこれらのうちの1つが1ならば g の長さを減らすことができる．もしHの位数がMで $n\geq M+2$ ならば，これらの表現のうちの1つが1になるか，同じ値が繰り返して現われるものがあるはずである．たとえば $h_2\cdots h_{2r}h_{2r+1}^{-1}\cdots h_3^{-1}=h_2\cdots h_{2r}\cdots h_{2s}h_{2s+1}^{-1}\cdots h_{2r+1}^{-1}\cdots h_3^{-1}$ とすると，$h_{2r+2}\cdots h_{2s}h_{2s+1}^{-1}\cdots h_{2r+3}^{-1}=1$ となり，これは h_{2r+2} の代りに置き換えられるものの1つである．同様にして，同じ値の中に $h_2h_4\cdots h_{2r}h_{2r-1}^{-1}\cdots h_3^{-1}$ がはいっているときも，h_{2r+1} が1と置き換えられる．いずれにせよ，$n\geq M+2$ ならば長さを減らすことができる．ゆえに任意の g は長さが $n\leq M+1$ の語で表わされ，$H\cup(x)$ の位数は高々 M^{M+1} である．

18.4. 制限された Burnside 問題．P. Hall と G. Higman の定理．$B(6, r)$ の有限性

次の命題は Burnside 予想のもう少し弱い形である．その証明は制限された Burnside 問題として知られている．

R_n：任意の正整数 r に対して，r 個の元で生成され，指数が n であるような任意の有限群の位数はたかだか $b_{n,r}$ であるというような整数 $b_{n,r}$ が存在する．

ある n の値に対して R_n が正しかったとしても，r 個の生成元をもつ指数 n の無限群が存在するかもしれない．しかし R_n が正しければ，r 個の元から生成される指数 n の有限群の中で最大のもの $R(n, r)$ が存在する．なぜなら，r 個の元から生成される指数 n の有限群は，r 個の生成元をもつ自由群を F_r

とするとき，F_r のすべての元の n 乗を含む適当な正規部分群 N_i をとれば，F_r/N_i という商群になるが，R_n が正しければ，このような正規部分群 N_i は有限個しか存在せず，それらの共通部分 N は有限指数で，$F_i/N=R(n,r)$ は r 個の生成元をもつ指数 n の有限群で，ほかのものはすべてこれの準同型像になるからである．

群 G の降中心鎖を

(18.4.1) $$G=G_1\supseteq G_2\supseteq G_3\supseteq\cdots$$

とする．$G_s=G_{s+1}$ という関係が成り立ったとしよう．すると，降中心鎖の性質から，$G_s=G_{s+1}=\cdots=G_{s+i}=\cdots$ となる．G が巾零群ならば，ある $G_{s+i}=1$ となるから，$G_s=1$ である．素数巾の指数 $n=p^t$ をもつ有限群 G は巾零だから，このような群においては $G_s=G_{s+1}$ ならば $G_s=1$ となる．さて，G の指数が p^t で r 個の元から生成されているとしよう．もしすべてのこのような群 G に対し，$G_s=G_{s+1}$ となる整数 $s=s(p^t,r)$ が存在することがいえれば，指数が $n=p^t$ に対する制限された Burnside 問題が解けたことになる．

$(xy)^n$ に集中過程（定理 12.3.1）を適用すると

(18.4.2) $$(xy)^n=x^ny^nc_1{}^{a_1(n)}\cdots c_t{}^{a_t(n)}$$

となることがわかる．ただし c_i の重さが m ならば，その指数 $a_i(n)$ は

(18.4.3) $$u_{i1}n+u_{i2}\binom{n}{2}+\cdots+u_{im}\binom{n}{m}$$

という形をしている．そして c_i が

(18.4.4) $$c_i=(y,\overbrace{x,\cdots,x}^{s})$$

という形をしていれば，指数 $a_i(n)$ は

(18.4.5) $$(y_{j_1},x_{j_2},x_{j_3},\cdots,x_{j_{s+1}})$$

において

(18.4.6) $$j_1<j_2<j_3<\cdots<j_{s+1},$$
$$1\leq j_k\leq n$$

となる添数 $j_1,j_2,\cdots,j_{s+1}$ の選び方の数であるが，これは $1,2,\cdots,n$ から $s+1$

個の異なる数を選ぶ方法の数だから $\binom{n}{s+1}$ となる．

もし $n=p$ が素数ならば，2項係数 $\binom{p}{i}$, $1\leq i\leq p-1$ はすべて p の倍数であるから，重さがたかだか $p-1$ の交換子に対しては，指数はすべて p の倍数になる．そして交換子

$$(y, \overbrace{x, \cdots, x}^{p-1}) \tag{18.4.7}$$

に対しては指数は $\binom{p}{p}=1$ となる．ゆえに指数 p の群 G においては

$$1=(xy)^p=\overbrace{(y, x, \cdots, x)}^{p-1}v_1\cdots v_t \tag{18.4.8}$$

となる．ただし $v_1, v_2, \cdots, v_t$ は重さが少なくとも p の交換子であって，重さが p の場合は y に関する重さが2以上である．

これより G_p における G_{p+1} を法とした関係

$$(y, \overbrace{x, \cdots, x}^{p-1})v_1\cdots v_s\equiv 1 \pmod{G_{p+1}} \tag{18.4.9}$$

が得られる．ただし $v_1, \cdots, v_s$ は x と y について重さ p の交換子で，x についての重さは少なくとも1でたかだか $p-2$ である．（10.2.1）という規則により，任意の群において，(u, v) の重さが m ならば

$$(u^i, v^j)\equiv(u, v)^{ij} \pmod{G_{m+1}} \tag{18.4.10}$$

が成り立つ．これを使うと，(18.4.9) における v の1つが x について重さ r だとすると，(18.4.9) において x を x^i で置き換えると，v は v^{i^r} に置き換わる．$i=1, \cdots, p-1$ と置いて，これを掛けた積における v の指数は，$1\leq r\leq p-2$ に対しては

$$1^r+2^r+3^r+\cdots+(p-1)^r\equiv 0 \pmod{p} \tag{18.4.11}$$

となるが，最初の項 $(y, \overbrace{x, \cdots, x}^{p-1})$ に対しては $r=p-1$ で $i^r\equiv 1 \pmod{p}$ である．ゆえに積は

$$(y, \overbrace{x, \cdots, x}^{p-1})^{p-1}\equiv 1 \pmod{G_{p+1}} \tag{18.4.12}$$

という形になり，したがって

(18.4.13) $$(y, \overbrace{x, \cdots, x}^{p-1}) \equiv 1 \pmod{G_{p+1}}$$

が成り立つ．この関係が素数指数 p の群についての制限された Burnside 問題を考える際の鍵となる．これから出発して Kostrikin [1] は 2 個の生成元をもつ指数 5 の群 G に対する制限された Burnside 問題を解いた．彼は $G_{13}=G_{14}$ となり，Gが有限群ならば位数はたかだか 5^{34} であることを示した．

制限された Burnside 問題の研究をした人は何人もいるが，群に付随した Lie 環において計算を行なった方が便利な場合がしばしばある．そこでこれについて述べることにしよう．

結合環Rにおいて **Lie 積** (Lie product) $[x, y]$ を

(18.4.14) $$[x, y]=xy-yx$$

という規則で定義する．Rにおける加法とこの Lie 積により，Rの元の全体は Lie 環Lをつくる．Lie 環Lは次の規則を満たす．

$L0$. 加法 $x+y$ と Lie 積 $[x, y]$ が定義されている．

$L1$. 加法に関しては，零元 0 をもつ可換群になる．

$L2$. $[x+y, z]=[x, z]+[y, z]$.

$[x, y+z]=[x, y]+[x, z]$.

$L3$. $[x, x]=0$.

$L4$. $[[x, y], z]+[[y, z], x]+[[z, x], y]=0$.

(18.4.14) により定義された $[x, y]$ が，これらの規則を満たすことは容易に確かめられる．

$L2$ と $L3$ より

(18.4.15) $$\begin{aligned}0=[x+y, x+y]&=[x, x]+[x, y]+[y, x]+[y, y]\\&=[x, y]+[y, x]\end{aligned}$$

となるから，

(18.4.16) $$[y, x]=-[x, y]$$

となることが分かる．Rが $x_1, \cdots, x_r$ という元で生成されているとき，$x_1, \cdots, x_r$ から加法と Lie 積 $[x, y]$ により生成される元の全体は，加法と結合積に

よって生成されるRの元を全部含むとは限らない．Lie 積によって生成される元は **Lie 元** (Lie element) とよばれる．x_1^2 は Lie 元とは限らないが，$x_1^2x_2-2x_1x_2x_1+x_2x_1^2=x_1(x_1x_2-x_2x_1)-(x_1x_2-x_2x_1)x_1$ は Lie 元である．もちろん，Rの関係によっては x_1^2 が Lie 元になることもある．

規則 $L0$, $L1$, $L2$, $L3$, $L4$ を Lie 環 L の定義とみることもできる．Garrett Birkhoff [1] と E. Witt [1] により，任意の Lie 環 L は，適当な結合環R の Lie 元全体のつくる環として表わされるということが示された．しかし，この重要な結果はここでは必要としない．

群Gの降中心鎖を

$$G=G_1\supseteq G_2\supseteq G_3\supseteq\cdots\supseteq G_n\supseteq\cdots \tag{18.4.17}$$

とするとき，G の**付随 Lie 環** (associated Lie ring) は次のようにしてつくられる．

1) L は加法的に書かれた商群 G_i/G_{i+1} のカルテジアン和であって，L の加法はこのカルテジアン和によって与えられる．

2) G_i/G_{i+1} の元は，i 次の同次元 (homogeneous element) とみなされる．

3) i 次の同次元 A と j 次の同次元 B との Lie 積は，G_{i+j+1} を法とした交換子 (A, B) とする．

4) Lの一般の元の Lie 積は（3）と分配律により与えられる．

これらの規則により本当に Lie 環が定義されるということは証明しないことにする．ただ $L2$ が交換子に関する等式 (10.2.1.2) と (10.2.1.3) に，$L4$ が (10.2.1.5) に対応するということだけ注意しておく．§11.2の結果を言い換えると，r 個の生成元をもつ自由群に対応する Lie 環は r 個の生成元をもつ自由 Lie 環になることが示される．ただし無限和も許しておく必要がある．§11.2の方法を少し変えると，これらの規則により Lie 環が定義されることを証明するのに使うことができる．

Lie 環Lにおける単項式を左正規化形式に書くことにする．すなわち，$[x_1, x_2]$ のことを x_1x_2 と書き，あとは帰納的に $[x_1\cdots x_{n-1}, x_n]$ のことを $x_1x_2\cdots x_n$

と書く．次の定理は Graham Higman [1] による．

定理 18.4.1. 素数指数 p の群の付随 Lie 環においては恒等式 $yx^{p-1}=0$ が成り立つ．

証：素数指数 p の群においては (18.4.13) という関係が成り立つ．これを

(18.4.18)
$$(y,\overbrace{x,\cdots,x}^{p-1})=c_1c_2\cdots c_t$$

という形に書くことにする．ただし $c_1,c_2,\cdots,c_t$ は x と y について重さ $p+1$ 以上，y については重さ 1 以上の交換子である．

ここで $x=x_1x_2\cdots x_p$ と置き，(10.2.1) という規則を使って，異なる x_i の交換子だけが左辺に残るように集めると

(18.4.19)
$$X=\prod_{\sigma}(y,x_{1\sigma},\cdots,x_{(p-1)\sigma})=d_1\cdot d_2\cdots d_s$$

となる．ただし σ は $1,2,\cdots,p-1$ についての $(p-1)!$ 個の置換をある順序にしたがって動き，$d_1,d_2,\cdots,d_s$ は y についての重さが正の交換子で，(1) $y,x_1,\cdots,x_{p-1}$ についての重さが $p+1$ 以上，または (2) $y,x_1,\cdots,x_{p-1}$ についての重さが p で，ある x_j は現われない．各 d_i は $y,x_1,\cdots,x_{p-1}$ のそれぞれについて重さが正だとしてよい．このことは帰納法により証明される．実際，上のような関係において各 d_i が $y,x_1,\cdots,x_{j-1}$ について正の重さをもつようにできたとする．さらに交換子を導入することにより，x_j に関して重さ 0 の d_i が最初の $d_1\cdots d_t$ だとしてよい．そこで $x_j=1$ と置くと $d_1d_2\cdots d_t=1$ となり，これらを除くことができる．ゆえに d_i は $y,x_1,\cdots,x_{p-1}$ のどれについても重さが正で，重さの合計は $p+1$ だとしてよい．最初の表現における重さ p の交換子はどれかの x_j がなかったわけだから，どこかの段階で除かれてしまっている．このことは，付随 Lie 環の言葉でいうと，$y,x_1,x_2,\cdots,x_{p-1}$ を任意の重さの同次元としたとき，

(18.4.20)
$$\sum_{\sigma}yx_{1\sigma}x_{2\sigma}\cdots x_{(p-1)\sigma}=0$$

となることを意味する．(18.4.20) は L において同次元 $y,x_1,\cdots,x_p$ について

成り立つ等式であるが，これは各変数について線形であるから，この等式は任意の変数について成り立つ．そこで $x_1=x_2=\cdots=x_{p-1}=x$，y は任意とすると，(18.4.20) は

$$(p-1)!yx^{p-1}=0 \tag{18.4.21}$$

となり，Lは標数 p であることが容易に分かるから，

$$yx^{p-1}=0 \tag{18.4.22}$$

となり，定理が証明された．

標数が 5（もっと正確には標数が 2, 3 と素）の Lie 環 L において $yx^4=0$ という関係が成り立つことを使って，Graham Higman [1] は，L が r 個の元から生成されるとき，Lにおける Nr 次以上の積は 0 になることを示した．ただしNは r に依存しない整数である．実際彼は $N=25$ としてこれを証明したが，もっと計算すれば，$N=9$ としてこの結果が証明できると思うと彼はいっているが，それにしても最良の評価かどうかはわからない．

Philip Hall と Graham Higman [1] の重要な論文において，一般の指数に対する制限された Burnside 問題を素数巾指数の場合に関連づけた．このためには有限可解群に制限することが必要になる．したがってこの場合の R_n よりも弱くなった予想は次の形になる．

S_n；各正整数 r に対し，r 個の元で生成される指数 n の有限可解群の位数はたかだか $b_{n,r}$ になるような整数 $b_{n,r}$ が存在する．

彼等の結果を正確な形でいうと，

定理 18.4.2. $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ で，$i=1,\cdots,s$ について $S_{p_i^{e_i}}$ が正しければ，S_n も正しい．

この定理の証明には，長い複雑な準備を必要とするので，ここでは証明は与えないことにする．位数 p^aq^b の有限群は可解だから（定理 16.8.7），n がたかだか 2 つの素数でしか割れないときは，R_n と S_n は同じ命題になる．そして Burnside 群 $B(2,r)$，$B(3,r)$，$B(4,r)$ は有限群になることは知られており，Graham Higman が R_5 の成り立つことを示したから，定理 18.4.2 により，

R_6, R_{12}, R_{10}, R_{15}, R_{20} そして S_{30}, S_{60} の成り立つことが分かる. これらの結果に勇気づけられ, 著者は $B(6,r)$ が有限群になることを証明した. その証明の概略を以下で与えることにしよう.

まず, Philip Hall と Graham Higman の結果の一部と, 残りの部分でやっていることの説明を与えることにする.

p を素数とするとき, 群の位数が p と素のとき p'-群, 位数が p 巾のとき p-群とよぶことにする.

定　義：有限群Gは, 正規鎖

(18.4.23) $$1=V_0\subset V_1\subset\cdots\subset V_n=G$$

で, 商群 V_{i+1}/V_i が p-群または p'-群となるものが存在するとき, **p-可解** (p-solvable) とよばれる.

定理 9.2.4 により, 有限可解群Gはすべての素数 p に対し p-可解となることを注意する. p-可解群Gに対し, **昇 p-鎖** (upper p-series)

(18.4.24) $$1=P_0\subseteq N_0\subset P_1\subset N_1\subset P_2\subset\cdots\subset P_l\subseteq N_l=G$$

を, N_k/P_k は G/P_k の最大正規 p'-部分群, P_{k+1}/N_k は G/N_k の最大正規 p-部分群となるように帰納的に決める. $N_l=G$ となる最小の整数 l をGの p-長さとよび, l_p または $l_p(G)$ と書く. l_p というのは, (18.4.23) のような V_{i+1}/V_i が p-群または p'-群になっているGの正規鎖に現われる p-商群の最小数であることが容易に分かる.

Hall-Higman の論文の目的は, p-可解群Gの p-長さとGの Sylow p-部分群 $S(p)$ の性質とを関連づけることである. 特に p^{e_p} を $S(p)$ の指数, すなわち $S(p)$ の元の位数の最大値とすると, Gの指数, すなわちGの元の位数の最小公倍数は $n=\prod_p p^{e_p}$ となる. 彼等の主定理は奇素数 p に対し適用され, $p=2^n+1$ という形をした Fermat 素数 p と Fermat 素数でない素数に対しては結果が少し異なる. Burnside 問題と関係するこの定理は,

定理 18.4.3. p が奇素数で, Gが p-可解群とすると,

1) p が Fermat 素数でなければ $e_p\geq l_p$,

2) p が Fermat 素数ならば $e_p \geq [\frac{1}{2}(l_p+1)]$.

定理 18.4.3 から定理 18.4.2 が容易に導かれる. $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ とする. n が偶数ならば $p_1=2$ にとれ, $m=p_1^{e_1}p_2^{e_2}\cdots p_{s-1}^{e_{s-1}}$ に対し S_m が正しいとして, s についての帰納法を行なう. 定理 18.4.3 により, 指数 n の有限可解群 G の p_s-長さ $l=l_{p_s}\leq 2e_s$ である. そこで G が r 個の元から生成されているとすると, S_m から G/P_l の位数は $b_{m,r}$ でおさえられ, また P_l の生成元の数も, たとえば r_1 でおさえられる(補題 7.2.2 の系). すると $S_{p_s^{e_s}}$ より P_l/N_{l-1} は位数も, N_{l-1} の生成元の数もおさえられる. これを繰り返せば, N_i/P_i も P_i/N_{i-1} も位数はある $b_{m,k}$ または $b_{p^{e_s},k}$ でおさえられ, $l\leq 2e_s$ だから, G の位数も有界であることが分かる.

定理 18.4.4. 有限 p-可解群 G の昇 p-鎖
$$1=P_0\subseteq N_0\subset P_1\subset N_1\subset P_2\subset\cdots\subset P_l\subseteq N_l=G$$
において, P_1/N_0 はその G/N_0 における中心化群を含む.

系 18.4.1. P_1 はその G における中心化群を含む.

系の証: x が G において P_1 を中心化したとすると, G/N_0 において xN_0/N_0 は P_1/N_0 を中心化する. ゆえに定理より xN_0/N_0 は P_1/N_0 にはいる. よって G において剰余類 xN_0 は P_1 に含まれ, x は P_1 に含まれる.

定理の証: N_0 は G の最大正規 p'-部分群だったから, $G_1=G/N_0$ には正規 p'-部分群は存在しない. つくり方より G_1 の部分群 $\bar{P}_1=P_1/N_0$ は G_1 の最大正規 p-部分群である. $\bar{P}_1$ の G_1 における中心化群を Z とし, 定理が成り立たない, すなわち $Z\not\subseteq\bar{P}_1$ とする. Z は G_1 の正規部分群だから, $Z\cup P_1=ZP_1$ は G_1 の正規部分群である. $Z\bar{P}_1\supset\bar{P}_1$ と仮定したから, M を $\bar{P}_1\subset M\subseteq Z\bar{P}_1$ となる G の極小正規部分群とする. $\bar{P}_1$ は G_1 の極大正規 p-部分群だったから, $M/\bar{P}_1$ は p-群ではない. G は p-可解だから $M/\bar{P}_1$ は p'-部分群である. ところが $\bar{P}_1$ と $M/\bar{P}_1$ は位数が互いに素だから, 定理 15.2.2 により M は $\bar{P}_1$ 上分解する. すなわち $M/\bar{P}_1$ と同型な M の部分群 K で, $M=K\bar{P}_1$, $K\cap\bar{P}_1$

$=1$ となるものが存在する. $K\subseteq Z\bar{P}_1$ だから, Kの元yによる $\bar{P}_1$ の変換は $\bar{P}_1$ の内部自己同型を引き起こすが, Kの位数と $\bar{P}_1$ の位数は互いに素だから, この内部自己同型は恒等写像でなければならない. ゆえにMはKと $\bar{P}_1$ の直積 $K\times\bar{P}_1$ となる. するとKはMの持性部分群になるから, G_1 の正規部分群になり, G_1 は正規 p'-部分群を含まないということに矛盾する. $Z\nsubseteq\bar{P}_1$ と仮定すると矛盾が導かれたわけで, これで定理が証明された.

次にやることは, 本質的には前定理の精密化である.

定理 18.4.5. Gを p-可解群, その p-昇鎖を

$$1=P_0\subseteq N_0\subset P_1\subset N_1\subset P_2\subset\cdots\subset P_l\subseteq N_l=G$$

とし, F/N_0 を P_1/N_0 の Frattini 部分群とすると, Gの元による変換が引き起こす P_1/F の自己同型は, G/P_1 を忠実に表現する.

証: F/N_0 は p-群 P_1/N_0 の極大部分群の共通部分で, P_1/F は基本可換 p-群である (定理 12.2.1). F/N_0 は P_1/N_0 の交換子群を含んでいるから, P_1 の任意の元が引き起こす P_1/F の自己同型は恒等写像になる. ゆえにGの元で, その変換により P_1/F の恒等自己同型を引き起こすものの全体はGの部分群(必然的にGの正規部分群となる)Kをつくり, $K\supseteq P_1$ となる. $K\supset P_1$ とすると矛盾が導かれることを示そう. そうすれば $K=P_1$ となり, G/P_1 は変換により P_1/F 上忠実に表現される. $K\supset P_1$ とすると, つくり方より P_1/N_0 は G/N_0 の極大正規 p-部分群だから, K/P_1 は p-群ではない. したがってKには P_1 にはいらない位数が p と素な元xで, P_1/F に恒等自己同型を引き起こすものがある. ところが定理 12.2.2 により, p-群 P_1/N_0 の自己同型で P_1/F 上恒等写像となるものの位数は p 巾である. ところがxの位数は p と素であるから, xは P_1/N_0 に恒等自己同型を引き起こすが, このことは定理 18.4.4 により $x\in P_1$ を意味する. これはxの選び方に矛盾する. $K\supset P_1$ とすると矛盾が導かれたわけだから, $K=P_1$ となり, 定理が証明された.

定理 18.4.5 により, G/P_1 は基本可換 p-群 P_1/F の変換により忠実に表現される. G/P_1 は p-可解群で, $l_p(G/P_1)=l_p(G)-1$ である. さらに定義

より G/P_1 は正規 p-部分群を含まない．Hall-Higman の論文の残りの部分では G/P_1 の P_1/F 上の表現を研究している．実際，これは p 個の元から成る体上のベクトル空間での線形変換による表現である．G/P_1 は p-可解群で，正規 p-部分群を含まない．この理論は，標数 p の体上の表現により忠実に表現されるこのような群についていえることに依存している．これらの結果には $l_p(G)=l_p(G/P_1)+1$ ということを使って，p-長さによる帰納法も行なっている．

結果を引用するのはこれぐらいにして，Burnside 群 $B(6,r)$ の性質を調べ，有限になることが示せるかどうかということに話を限ろう．

定理 18.4.6. 指数6の有限群 G においては，$l_2(G)\leqq 1$ および $l_3(G)\leqq 1$ が成り立つ．

証：指数6の有限群 G の位数は 2^a3^b であるから可解群である．G の昇 2-鎖において，P_1/N_0 は 2-群で G/N_0 における自分の中心化群を含んでいる．ところが G は指数6だから G の Sylow 2-部分群は指数2，したがって基本可換群である．ゆえに P_1/N_0 はそれを含む G/N_0 の Sylow 2-部分群により中心化される．ゆえに P_1/N_0 は G/N_0 の Sylow 2-部分群で，$l_2(G)=1$ となり，G の昇 2-鎖は

(18.4.25) $$1=P_0\subseteq N_0\subset P_1\subseteq N_1=G$$

という形になる．ただし N_0/P_0 は 3-群，P_1/N_0 は 2-群，N_1/P_1 は 3-群である．

(18.4.25) は G の正規鎖で，3-群となる商群はたかだか2つだから $l_3(G)\leq 2$ である．$l_3(G)=2$ ならば，G は位数9の元を含み，G の指数が6であるという仮定に反することを示そう．G の昇 3-鎖は

(18.4.26) $$1=A_0\subseteq B_0\subset A_1\subset B_1\subset A_2\subseteq B_2=G$$

という形をしている．ただし B_0/A_0, B_1/A_1, B_2/A_2 は 2-群，A_1/B_0, A_2/B_1 は 3-群である．

(18.4.27) $$1=B_0/B_0\subset A_1/B_0\subset B_1/B_0\subset A_2/B_0\subseteq G/B_0$$

は G/B_0 の昇 2-鎖で，その 2-長さは 1 だから，$A_2=B_2=G$ となることを注意しておく．定理 18.4.4 により，2-群 B_1/A_1 は A_2/A_1 における自分自身の中心化群となっている．ゆえに A_2/A_1 においては，位数 3 の元 x が与えられると，x と可換でない位数 2 の元 u が B_1/A_1 に存在する．そこで

(18.4.28) $$u=u_1,\quad x^{-1}u_1x=u_2,\quad x^{-1}u_2x=u_3$$

と置くと，$x^3=1$ だから $x^{-1}u_3x=u_1$ となる．$y=y_1=u_1u_2$，$y_2=u_2u_3$ と置く．u_1, u_2, u_3 は基本可換 2-群に属するから，$u_3u_1=(u_1u_2)(u_2u_3)=y_1y_2$ となる．ゆえに群 $C=\{x, y_1, y_2\}$ は

(18.4.29) $$x^3=1,\quad {y_1}^2={y_2}^2=1,\quad y_2y_1=y_1y_2,$$
$$x^{-1}y_1x=y_2,\quad x^{-1}y_2x=y_1y_2$$

という関係を満たす．x は u_1 と可換でないから $u_1\neq u_2$ で，したがって $y=u_1u_2\neq 1$ である．また $y_2=y_1$ とすると $x^{-1}y_2x=1$ となり，$1=y_2=y_1$ となる．ゆえに $y_2\neq y_1$ で，群Cは (18.4.29) という関係より位数が12で，実際，4 文字の上の交代群と同型であることが分かる．定理 18.4.5 より，F/B_0 を A_1/B_0 の Frattini 部分群とすると，G/A_1 は基本可換 3-群 A_1/F の変換により忠実に表現される．特にCは $A_1/F=W$ の変換により忠実に表現される．Wを加法的に書くと，G/A_1 の元 z によるWの変換は z を右作用素として表現される．そしてCだけでなく群環 C^* もWに作用している．Wのすべての元を 0 に写す C^* の元の全体は容易に分かるように C^* の両側イデアルをつくる．Cを

(18.4.30) $$x^3=1,\quad y^2=1,\quad (xy)^3=1$$

という関係により x, y により生成されているとみなす．すると $1+x+x^2$ を含む C^* の両側イデアルは

(18.4.31) $$x^2y(1+x+x^2)yx-(1+x+x^2)y-y(1+x+x^2)$$
$$+xy(1+x+x^2)yx^2=2-2y$$

も含む．すべての $w\in W$ に対して $w(1+x+x^2)=0$ となったとすると，(18.4.31) により $w(2-2y)=0$ となり，W の元は位数 3 だからすべての $w\in W$ に対し $wy=w$ となり，y が $W=A_1/F$ の変換として忠実に表現され

なくなり，定理 18.4.5 に反する．ゆえにある $w\in W$ に対し $w(1+x+x^2)\neq 0$ となる．乗法的な形でいうと，A_2/A_1 の元 x の剰余類 $\bar{x}A_1$ の代表元 $\bar{x}$ に対して

$$w(\bar{x}^{-1}w\bar{x})(\bar{x}^{-2}w\bar{x}^2)\neq 1 \tag{18.4.32}$$

となることを意味する．これは

$$(w\bar{x}^{-1})^3\bar{x}^3\neq 1 \tag{18.4.33}$$

ということだが，$\bar{x}^3$ および $(w\bar{x}^{-1})^3$ はともに W の元である．(18.4.33) により，これらのうちの少なくとも一方は単位元ではない．ゆえに $\bar{x}$ か $w\bar{x}^{-1}$ は位数が 9 である．したがって $l_3(G)=2$ とすると位数 9 の元が存在することになり，G が指数 6 という仮定に反する．ゆえに $l_3(G)\leq 1$ となり，定理が証明された．

定理 18.4.6 を使うことにより，r 個の元から生成される指数 6 の最大の有限群の正確な位数を求めることができる．

定理 18.4.7. $R(r,6)$ の位数は

$$2^a 3^{b+\binom{b}{2}+\binom{b}{3}} \tag{18.4.34}$$

である．ただし

$$a=1+(r-1)3^{r+\binom{r}{2}+\binom{r}{3}},\quad b=1+(r-1)2^r$$

である．

証：F_r を r 個の生成元をもつ自由群とする．F_r の元の平方全体で生成される部分群を S とすると，F_r/S は位数 2^r の基本可換群である．ゆえに定理 7.2.8 により，S は $b=1+(r-1)2^r$ 個の生成元をもつ自由群である．S の元の 3 乗全体で生成される S の全不変部分群を T とすると，S/T は $B(3,b)$ だから，T の S における指数は $3^{b+\binom{b}{2}+\binom{b}{3}}$ である．$g\in F_r$ ならば $g^2\in S$，よって $(g^2)^3\in T$ だから，F_r/T は指数 6 の有限群である．同様に F_r の元の 3 乗で生成される部分群 C は，F_r の指数 $3^{r+\binom{r}{2}+\binom{r}{3}}$ の部分群で，定理 7.2.8 により，C は $a=1+(r-1)3^{r+\binom{r}{2}+\binom{r}{3}}$ 個の自由生成元をもつ．C の元の 2 乗全

体で生成される全不変部分群DのCにおける指数は 2^a である．そこで $X=D\cap T$ と置く．任意の $g\in F_r$ に対し，DもTも g^6 を含むから，F_r/X は指数6の有限群である．F_r/X の昇 2-鎖は

(18.4.35) $$1=X/X\subset D/X\subset C/X\subset F_r/X$$

で，F_r/X の昇 3-鎖は

(18.4.36) $$1=X/X\subset T/X\subset S/X\subset F_r/X$$

であることが容易に分かる．そして C/D は F_r/X の Sylow 2-部分群と同型で，S/T は Sylow 3-部分群と同型である．したがって F_r/X の位数は（18.4.34）で与えられる．

Gをr個の元で生成される指数6の任意の有限群とする．Gの昇 3-鎖を

(18.4.37) $$1=P_0\subseteq N_0\subseteq P_1\subseteq N_1=G$$

とすると，N_1/P_1 の位数はたかだか 2^r であることが分かり，P_1 はたかだかb個の元で生成される．よってGの Sylow 3-部分群に同型な P_1/N_0 の位数はたかだか $3^{b+\binom{b}{2}+\binom{b}{3}}$ である．同様にGの位数はたかだか 2^b でしか割れない．

指数6に対する Burnside 予想の証明は長い計算を含んでおり，完全な証明を与える余裕はない．証明はいままでの結果には依存せず，$B(6,r)$ の位数を割る2巾が正確に与えられる．しかし3の巾を正確に求めるには定理 18.4.7 を使う必要がある．指数6の有限生成群Gの 2-長さは1で，$B(2,r)$ と $B(3,r)$ の有限性より有限群となる．これには正規鎖

(18.4.38) $$G\supset M\supset M'\supset 1$$

で，G/M は有限 3-群，M/M' は有限 2-群で，M'は指数3の有限生成群，したがって有限群になるようなものが存在することを示すという形をとる．ほとんどすべての困難はM'が指数3であることを示すところである．

定理 18.4.8. *r個の元から生成される指数6の群Gは有限群である．*

系 18.4.2. *$B(6,r)$ の位数は（18.4.34）で与えられる．*

補題 18.4.1. *Gの元の3乗全体は指数がたかだか $3^{r+\binom{r}{2}+\binom{r}{3}}$ の正規部分群*

Mを生成する.

補題 18.4.2. Mは位数2の元有限個で生成される. Mの交換子群M'のMにおける指数は2巾で, $abab$ という形の元有限個で生成される. ただし $a^2=b^2=1$ である.

補題 18.4.3. 群Hが $x_1, \cdots, x_n$ で生成され, x_i のうちの4つで生成されるHの部分群はすべて指数が3ならば, Hも指数3である.

補題 18.4.4. $H=\{a, b, c, d\}$ は指数6で, $\{a, b, c\}$, $\{a, b, d\}$, $\{a, c, d\}$ および $\{b, c, d\}$ は指数が3ならば, Hも指数3である.

補題 18.4.5. $H=\{x, a, b\}$ は指数6で, $x^2=1$, $a^3=b^3=1$, $xax=a^{-1}$, $xbx=b^{-1}$ ならば, $\{a, b\}$ は指数3である.

これは一番むずかしい補題で, 関係式についての複雑な計算を含んでいる.

補題 18.4.6. $H=\{x, a, b\}$ は指数6で, $x^2=1, a^3=b^3=1, xax=a^{-1}, xbx=b$ ならば, $\{a, b\}$ は指数3である.

補題 18.4.7. $H=\{x, a, b, c\}$ は指数6で, $x^2=1$, $a^3=b^3=c^3=1$, $xax=a^{-1}$, $xbx=b^{-1}$, $x\subset x=c^{-1}$ ならば, $\{a, b, c\}$ は指数3である.

補題 18.4.8. $H=\{x, a_i\} i=1, \cdots, n$ は指数6で, $x^2=1$, $a_i^3=1$, $xa_ix=a_i^{-1}$, $i=1, \cdots, n$ ならば, $\{a_i\}$ $i=1, \cdots, n$ は指数3である.

これは補題18.4.3, 4, 7から導かれることが容易に分かる.

補題 18.4.9. $H=\{a, b, c\}$ は指数6で, $a^2=b^2=c^2=1$ ならば, H' は指数3である.

補題 18.4.10. $H=\{a, b, c, d\}$ は指数6で, $a^2=b^2=c^2=d^2=1$ ならば, $\{abab, cdcd\}$ は指数3である.

補題 18.4.11. $H=\{a, b, c, d, e, f\}$ は指数6で, $a^2=b^2=c^2=d^2=e^2=f^2=1$

ならば, $\{abab, cdcd, efef\}$ は指数3である.

補題 18.4.12. M' は指数3で, 有限群となる. ゆえに G も有限群である.

この補題は補題 18.4.2, 3, 4, 11 からただちに得られる.

第19章　部分群の作る束

19.1. 一般的性質

群Gの部分群全体からなる集合 $L(G)$ において，部分群の結び（union）および共通部分（intersection）をとるという２つの演算を考えることによって，$L(G)$ に束の構造がはいる．位数が素数の巡回群Gに対しては，$L(G)$ は，全体群と単位群の２元からできており，したがってこれらの位数素数の巡回群の作る束はすべて互いに同型である．逆に $L(G)$ が，全体群Gおよび単位群の２元のみからなるような群Gは，単位群以外の位数が素数の巡回群に限ることを既に証明した（定理 1.5.4）．また位数 pq の非アーベル群（ただし，$p<q$, $p|q-1$）と位数 p^2 の初等アーベル群の作る束は同型である．すなわち単位群，$q+1$ 個の位数素数の巡回群および全体群からなる．このとき，任意の二つの相異なる真部分群をとってくれば，共通部分は単位群に一致し，また，結びは全体群に一致する．群Gによって束 $L(G)$ は一意的に定まるが，一般には，束 $L(G)$ からGが一意的に定めるとは限らない．また，いかなる群Gをとってきてもそれから作られる束$L(G)$に一致しないような束Lの例も容易に作ることができる．しかし，多くの群Gは$L(G)$によって一意的に決定される．たとえば，四次交代群，四次対称群の作る束に関してはこのことが成り立つ．さらには，少数の比較的簡単な群を除いては$L(G)$がGを一意的に決定するということも正しいであろう．

束論の言葉でいうと，$L(G)$ は完備である．すなわち，無限個の元の最大下界，および最小上界が常に存在する．なぜならば，ある部分群の集合にふくまれているすべての部分群に共通な元からなる集合はまたGの部分群をなし，あきらかにこの部分群の集合の最大下界になっている．また，同様にしてある部分群の集合にふくまれている部分群全体が生成する部分群はあきらかにこの部

分群の集合の最小上界になっているからである．

部分群の作る束についてのさらに詳しい研究に関しては Suzuki [1] を参照．

19.2. 局所巡回群と分配束

束においては，次の2つの分配則 $D1$, $D2$ は互いに同値である．

$D1$. $a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$

$D2$. $a\cup(b\cap c)=(a\cup b)\cap(a\cup c)$

$D1$ から $D2$ は次のようにして導くことができる．$D1$ によって，

$$\begin{aligned}(a\cup b)\cap(a\cup c)&=[(a\cup b)\cap a]\cup[(a\cup b)\cap c]\\&=a\cup[(a\cap c)\cup(b\cap c)]\\&=[a\cup(a\cap c)]\cup(b\cap c)\\&=a\cup(b\cap c)\end{aligned}$$

となり，すなわち $D2$ が得られた．同様にして $D2$ から $D1$ が導かれる．束において，この分配則は非常に強い条件である．すなわち，群 G の束 $L(G)$ が分配則を満たせば，G が局所巡回群でなければならない．このことをこれから証明しよう．

定　義：群 G が局所巡回群であるとは群 G の任意の有限個の元から生成される部分群が巡回群であることと定義する．(§13.1の定義と比較)

局所巡回群の単位元と異なる各元の位数はすべて有限であるか，すべて無限であるかのいずれかである．なぜならば，単位元と異なる2つの元の位数がおのおの有限と無限であったとすれば，この2つの元から生成される群は巡回群になり得ないからである．有理数の作る加法群 R_+ は非周期的な（単位元でない各元の位数が無限な）局所巡回群であり，一方，R_+ を法1で考えた群 (R_+/Z) は周期的な（各元の位数が有限な）局所巡回群である．任意の局所巡回群はこれ等二つの群のいずれかの部分群になっていることを示すことはさほどむずかしくはないがここでは省略する．

定理 19.2.1. 束 $L(G)$ が分配束であることは群Gが局所巡回群であるための必要十分条件である.

証：（必要条件）　G を局所巡回群とする．A, B, C を G の 3 つの部分群とし，分配則 $D1$ が成立することを示す.

$$A\cap(B\cup C)=U$$

$$(A\cap B)\cup(A\cap C)=V$$

と置く.

一般に

$$A\geqq A\cap B$$

$$B\cup C\geqq B\geqq A\cap B$$

であるから

$$U=A\cap(B\cup C)\geqq A\cap B$$

が得られる.

同様に

$$A\geqq A\cap C$$

$$B\cup C\geqq C\geqq A\cap C$$

であるから

$$U=A\cap(B\cup C)\geqq(A\cap B)\cup(A\cap C)=V$$

が成り立つ.

したがって, $U\leqq V$ を証明すれば, 必要条件の証明は完成する．U から元 g を任意にとってくる．このとき g は，群G がアーベル群でありしたがって $B\cup C=BC$ であることから,

$$g=a=bc \qquad a\in A,\ b\in B,\ c\in C$$

と表わされる．G は局所巡回群であるから元 b と c は巡回群 $\{u\}$ を生成し，したがって，整数 r, s, m, n が存在して $u^r=b$, $u^s=c$, $b^mc^n=u$ と表わされる．したがって，$u^{rm+sn}=u$ が得られる．一方，$a=bc=u^{r+s}$ である．さて，$x=u^{r(r+s)}=a^r=b^{r+s}\in A\cap B$, $y=u^{s(r+s)}=a^s=c^{r+s}\in A\cap C$ であるから $a=u^{r+s}=u^{mr(r+s)+ns(r+s)}=x^my^n\in(A\cap B)\cup(A\cap C)=V$ したがって，$U\leqq V$

が得られ，必要条件の証明は完成した．

（十分条件）$L(G)$ が分配束である．すなわち分配則 $D1$, $D2$ を満たすとし，G が局所巡回群であることを示す．b, c を G の任意の二元とし $a=bc$, $A=\{a\}$, $B=\{b\}$, $C=\{c\}$ とする．$a\in B\cup C$ であるから

$$A=A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$$

が成り立つ．$A\cap B$, $A\cap C$ は巡回群の部分群であるから巡回群で，$A\cap B=\{u\}$, $A\cap C=\{v\}$ と表わされる．さらに適当な自然数 x, y, z, w が存在して，$a^x=b^y=u$, $a^z=c^w=v$ と表わされる．u, v は共に a の巾であるから可換で，また，$A=\{u\}\cup\{v\}$ であるから，$a\in A$ は $a=u^r v^s=v^s u^r$ と表わされる．さらに，$a=bc$ であったから，$bc=u^r v^s=b^{yr}c^{ws}=c^{ws}b^{yr}$ と表わされる．したがって，$b^{1-yr}=c^{ws-1}$，したがって，$c^{-ws+1}=b^{yr-1}$，すなわち $v^{-s}c=u^r b^{-1}$．したがって，$cb=v^s u^r=u^r v^s=bc$ が成り立ち，b と c は可換であるから G は可換群になる．

次に，群 G に位数有限の元 $a\neq 1$ と位数無限の元 b は共に含まれ得ないことを示す．もし，このような a, b があるとすると，$c=ab$ と置くと c の位数は無限で $a=b^{-1}c$ であるから $\{a\}=\{a\}\cap(\{b\}\cup\{c\})$ が成り立つ．一方，無限巡回群 $\{b\}, \{c\}$ は位数有限の元 $\neq 1$ を含まないので，

$$\{a\}\cap\{b\}=1,\quad \{a\}\cap\{c\}=1$$

であるから，$(\{a\}\cap\{b\})\cup(\{a\}\cap\{c\})=(1)\cup(1)=1\neq\{a\}$ が得られ分配則 $D1$ と矛盾する．したがって以下 G が非周期的な場合と G が周期的な場合のそれぞれについて別々に考えればよい．G が非周期的な場合，二元 b, c から生成される群が巡回群でないとすると，可換群の基本定理から b, c は巡回群の直積 $\{b\}\times\{c\}$ を生成する．$a=bc$, $A=\{a\}$, $B=\{b\}$, $C=\{c\}$ と置くとき，$A=A\cap(B\cup C)$, $(A\cap B)\cup(A\cap C)=(1)\cup(1)=(1)$ で分配則 $D1$ が成り立たなくなり仮定に矛盾する．したがって，G の任意の二元 b, c は巡回群を生成する．G が周期的な場合，二元 b, c の位数が互いに素とすると $\{b\}\cup\{c\}=\{bc\}$ であるから b, c は巡回群を生成する．しかし b, c の位数が公約数（たとえば素数 p）を持つときは分配則は成り立たなくなる．なぜならば，位数

p の元 $b_1 \in \{b\}$, $c_1 \in \{c\}$ をとってきて，$a_1 = b_1 c_1$, $A = \{a_1\}$, $B = \{b_1\}$, $C = \{c_1\}$ と置くとき，分配則 $D1$ が成り立たないからである．したがって，Gが非周期的，周期的いずれの場合も $L(G)$ が分配則を満たすためには，Gの任意の二元は巡回群を生成しなければならない．このことから任意の有限個の元は巡回群を生成しなければならないことはただちに分かる．したがってGは局所巡回群であり，十分条件の証明が完成した．

19.3. 岩沢の定理

群Gの各組成列（または主組成列）の長さはすべて同じであることを§8.4で示した．この性質は群Gの正規部分群の作る束が Modular 束であることおよび組成列の束が弱い形での Modular 律を満たすことに負っている．しかし，一般には，束 $L(G)$ の極大鎖の長さは一定ではない．定理10.5.5で，超可解群Gにおいては，$L(G)$ の極大鎖の長さは一定であることを示した．次の定理はこの逆が成り立つことを主張する．(Iwasawa [1])

定理 19.3.1. 有限群Gが超可解群であるための必要十分条件は，束 $L(G)$ の極大鎖の長さが一定であることである．

証：(必要条件) 先に述べたように，定理10.5.5により極大鎖の長さは一定で，この長さは群Gの位数を割る素数の個数（繰り返しを含めた）であることが証明ずみである．

束のすべての極大鎖の長さが常に一定であるとき，その束は**等鎖条件**を満たすとよぶことにする．束 $L(G)$ が等鎖条件を満たせば，明らかにGの部分群Hの作る束 $L(H)$ およびGの商群 G/N の作る束 $L(G/N)$ も等鎖条件を満たす．

(十分条件) Gは有限群で $L(G)$ は等鎖条件を満たすと仮定する．束 $L(G)$ の長さが1になるような群Gは位数が素数の巡回群であるから超可解である．したがって，束 $L(G)$ の長さに関する帰納法を用いて証明する．すなわち，Gのすべての部分群および商群が超可解群であると仮定してよい．さて，超可解群に関する次の補題が必要とされる．

補題 19.3.1. Gを位数 $n=p_1p_2\cdots p_m$ $p_1\leqq p_2\leqq\cdots\leqq p_m$（各 p_i は素数）の超可解群とすれば，Gは商群 K_i/K_{i-1} の位数が $p_{m-i+1}(i=1,\cdots,m,)$ であるような主組成列

$$K_0=1\subset K_1\subset K_2\subset\cdots\subset K_m=G$$

を持つ.

証：系10.5.2から明らか.

次に，Gが正規部分群を持つことを示そう．これが証明の一番主要な部分である．このとき，次の補題を必要とする.

補題 19.3.2. Gが位数が素数pで割れる有限群であれば，次の（1），（2）のいずれかが成り立つ.

（1） Gはp正規である.

（2） Gは，1つの Sylow p-部分群 $S_1(p)$ の正規部分群であり，ほかのもう1つの Sylow p-部分群 $S_2(p)$ の正規部分群でないような p-群Pを部分群に持つ.

証：G が p-正規であるとは，ある1つの Sylow 部分群 $S_1(p)$ の中心 Z が，Zを含むほかの任意の Sylow 群 $S_2(p)$ の中心であることと定義したことを思い出そう．したがって，Gが p-正規でないならば，ある Sylow 部分群 $S_1(p)$ と $S_2(p)$ が存在して，$S_2(p)$ は $S_1(p)$ の中心Zを含むがZは $S_2(p)$ の中心にはならない．ここでは（1）でない，すなわちGは p-正規でなければ $P=Z$ とおいたとき，（2）が成立することを示す．もし，Zが$S_2(p)$の正規部分群であると仮定すれば，$S_1(p)$，$S_2(p)$ は共に $N=N_G(Z)$ に含まれる．したがって $S_1(p)$, $S_2(p)$ は共にNの Sylow 部分群と考えられるからNにおいて共役である．すなわち $x\in N$ が存在して $x^{-1}S_1(p)x=S_2(p)$ となる．Zは $S_1(p)$ の中心であるから，$S_2(p)=x^{-1}S_1(p)x$ の中心は $x^{-1}Zx$ であるが，$x\in N_G(Z)$ であるから $x^{-1}Zx=Z$ となり，Z は $S_2(p)$ の中心となり，仮定に反する．したがって，補題の証明が完成した.

さて，定理の証明にもどろう．いま，群Gの位数が $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ で $p_1\lneqq p_2\lneqq\cdots\lneqq p_r$ は異なる素数であると仮定する．最初の目標は，nを割る最小の素数 p_1 に対して補題19.3.2における（2）の場合が成り立っていれば，Gは正規部分群を持つことを示すことである．Burnside の定理4.2.5により $t\not\equiv 0\pmod{p_1}$ 個の p_1-群 $h_1,\cdots,h_t$ が存在し，それらはそれらの合併Hにおいておのおの正規でかつHのGにおける正規化群 $N=N_G(H)$ においておのおのが共役になる．HがGの正規部分群であればGには正規部分群が存在することになり目標は達成される．NがGの真部分群であると仮定すると，Nは帰納法の仮定により超可解群になる．補題19.3.1をNに適用すれば，Nにおける指数が$|N|$を割る最小の素数 p_1 の最高巾となるNの正規部分群Qが存在することが分かる．したがってQとHは共にNの正規部分群であり，$Q\cap H=1$（なぜならHは p_1-群）であるから $Q\cup H=Q\times H$ となり，QはHの各元と可換になる．したがって，群 h_1 の正規化群は p_1 と素な指数 t を持つことができない．これは t のとり方に矛盾する．以上のことから，Gが正規部分群を持たなければ，NはGの真部分群でなく，したがって（2）の場合は起こらない．したがって最初の目標の証明は完了した．

次に（1）の場合を考えよう．すなわち，Gは p_1-正規であるとする．Zを一つの Sylow 部分群 $S_1(p_1)$ の中心とし，$K=N_G(Z)$ と置く．もし $K=G$ であればZはGの正規な真部分群である．以下KはGの真部分群であると仮定する．このとき，帰納法の仮定により，K は超可解群である．補題19.3.1をKに適用すれば，Kは指数 p_1 の正規部分群Wを持たなければならない．K/Wは位数 p_1 の巡回群であるから，$W\supseteq K'$（Kの交換子群）となり，Kは可換 p_1-群である自明でない準同形像を持つ．この準同形像を $K/K'(p)$ で表わす．Gは p_1-正規であるから，このとき定理14.4.5を適用すれば，$G/G'(p_1)$は $K/K'(p_1)$ と同型になり，したがって $G'(p_1)$ はGの正規な真部分群になる．したがって，すべての場合にGは正規な真部分群を持つことが証明できた．したがって帰納法の仮定により，その正規部分群およびGのそれによる商群は超可解であるからGは可解であることが結論できる．

いま，Gの位数を$n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$，$p_1\lneqq p_2\lneqq\cdots\lneqq p_r$，$m=e_1+e_2+\cdots+e_r$とすると，$G$は可解であることから極大鎖の長さは$m$である．$S(p_r)$を位数$p_r^{e_r}$の Sylow 群とし，$1\subset A_1\subset A_2\subset\cdots\subset A_{e_r}=S(p_r)\subset B_1\subset\cdots\subset B_{m-e_r}=G$を極大鎖とする．$S(p_r)$が$G$の正規部分であることを示すことが以下の目標である．さて，$B_1/S(p_r)$の位数はある素数$p_j(<p_r)$である．B_1における$S(p_r)$に共役な部分群の個数は Sylow の第三定理により$1+kp_r$の形であり，また，この個数はp_jを割らなければならないので1でなければならない．すなわち，$S(p_r)\lhd B_1$である．同様にして，もし$S(p_r)\lhd B_i$であれば，B_{i+1}における$S(p_r)$に共役な部分群の個数は$1+kp_r$の形であり，また$[B_{i+1}:B_i]=p_j(<p_r)$を割らなければならないので1でなければならない．すなわち，$S(p_r)\lhd B_{i+1}$が得られる．したがって帰納法により$S(p_r)\lhd G$が得られた．Gは可解群だから，定理9.3.1により，位数$p_1^{e_1}\cdots p_{r-1}^{e_{r-1}}$の Sylow 補群$C$を持つ．$Z$を$S(p_r)$の中心とするとき，$Z$は$S(p_r)$の特性部分群であるから，$G$の正規部分群である．したがって，$C\cup Z=CZ=U$と置くと$C$の極大鎖は，$U$において$U$の極大鎖に拡張できる．したがって，$C\subset V$，$[V:C]=p_r$となる（$G$の）部分群$V$が存在する．$S(p_r)\lhd G$を示したのと同じ論法により，$V$は位数$p_r$の正規部分群$R$を持つことが分かる．一方$R$は$Z$に含まれなければならないので，$R$は$U$における唯一の Sylow p_r-部分群である．したがってRはCによって正規化され，$S(p_r)$の中心に属し，したがってRはGで正規である．帰納法により，G/Rは超可解群であるから，Gも超可解群になる．したがって，岩沢の定理の証明が完成した．

第20章　群論と射影平面

20.1. 射影平面の公理系

点の集合と，その部分集合（直線とよぶ）からなる集合との組で，次の公理 $P1\sim P3$ を満たすものを**射影平面**とよぶ.

$P1$. 任意の相異なる２点に対して，それ等を共に含む直線がただ一つだけ必ず存在する.

$P2$. 任意の相異なる２直線に対して，それ等に共に含まれる点がただ一つだけ必ず存在する.

$P3$. ４つの点でそのうちのどの３つも同一直線に含まれないようなものが存在する.

相異なる２点 A, B を含むただ一つの直線を，AとBを**結ぶ**直線とよび，相異なる２直線 k, t に同時に含まれるただ一つの点を，k, t の**交点**とよぶ．また（$P3$）を満たす４点のことを“一般の位置にある”ということにする.

一般の位置にある４点 A_1, A_2, A_3, A_4（この４点の存在は（$P3$）により保証されている）に対して，これ等のうちの２点づつを結ぶことにより次の６直線が得られる.

$$L_1 : A_1A_2B_1.$$
$$L_2 : A_1A_3B_2.$$
$$L_3 : A_1A_4B_3.$$
$$L_4 : A_2A_3B_3.$$
$$L_5 : A_2A_4B_2.$$
$$L_6 : A_3A_4B_1.$$

ここで B_1, B_2, B_3 はこれ等の直線の交点であるが，これ等６直線はすべて相異なっていなければならないから，各 B_i は $B_j(j\neq i)$ および $A_k(k=1, 2, 3, 4)$

と異なる.

補題 20.1.1. 任意の直線は少なくとも3点を含む.

証：上で定めた各直線 $L_1, \cdots, L_6$ は少なくとも3点を含む. それら以外の直線 L は, もし $A_1 \notin L$ ならば L_1, L_2, L_3 と相異なる3点で交わり, もし $A_2 \notin L$ ならば L_1, L_4, L_5 と相異なる3点で交わる. また $A_1 \in L$, $A_2 \in L$ ならば $L = L_1$ となり3点 A_1, A_2, B_1 を含む. 証終.

補題 20.1.2. 4直線でそのうちのどの3直線も一点で交わらないようなものが存在する.

証：L_1, L_2, L_5, L_6 はこの性質を満たす. 証終.

もし, 点と直線の役割を交換し“含む”と“含まれる”とを入れ換えれば, $P1$ と $P2$ は入れ換わり, また $P3$ と補題 20.1.2 は入れ換わる. このようにして, **双対性**の概念が導き出される. もう少し正確にいえば, 射影平面 π の双対平面 π^* は次のようにして構成される.

射影平面 π の点の集合を $\{P_i\}$, 直線の集合を $\{k_i\}$ とする. π^* の直線の集合として, $\{P_i\}$ と 1:1 に対応のつく集合 $\{p_i\}$, 点の集合として $\{k_i\}$ と 1:1 に対応のつく集合 $\{K_i\}$ をとり, $P_i \ni k_j$ の代わりに $p_i \in K_j$ ($k_j \rightleftarrows K_j$, $P_i \rightleftarrows p_i$) をとれば, π^* は射影平面になる（すなわち3つの公理を満たす）. さらに π^* の双対平面は π と一致する.（すなわち $(\pi^*)^* = \pi$）. このようにして, 点と直線, 含む, 含まれるの関係を入れ換えることにより, π に関する各命題は π^* に関する命題としていい直すことができる. このことを**双対の原理**とよぶ. 双対の原理により, π に関する命題が正しければ, π^* に関するその双対命題も正しいから, 補題 20.1.1 から次の補題が得られる.

補題 20.1.3. 任意の点は少なくとも3個以上の直線に含まれる.

なお, ここで与えた射影平面の公理系は, Veblen-Young “Projective Geometry”, vol. 1, page 16—18 の射影幾何の公理系（の平面の場合）と同値

である．この証明は読者に委ねる．

射影平面 π の1つの直線 L_1 が有限個の，たとえば $n+1$ 個の点を含むと仮定する．このとき，π の任意の直線が同一の個数（$n+1$ 個）の点を含むことを以下で示す．補題20.1.1により $n\geqq 2$ であり，公理（$P3$）により L_1 上にない相異なる2点，たとえば P_3 と P_4 が存在する．直線 P_3P_4 と L_1 との交点を B_1, P_1 と P_2 を L_1 上にある B_1 以外の互いに相異なる2点とすれば，直線 P_1P_3 と P_2P_4 の交点 B_2 は L_1 上および P_3P_4 上にはない．一方 L_1 上にない任意の点 P に対して，P と L_1 の各点を結ぶ $n+1$ 個の直線が得られるが，P を通る任意の直線は L_1 と交わらなければならないから，P を通る直線はそれら $n+1$ 個のものでつきる．特に P_3, P_4, B_2 はいずれも L_1 上にないから，それらの1点に対してその点を通る直線は全部で $n+1$ 個である．このとき P を通らない任意の直線 L は点 P を通る $n+1$ 個の直線と $n+1$ 個の点で交わり，L 上の点はそれら $n+1$ 個で全部である．一方 P_3, P_4, B_2 のいずれか1つは L 上にないから π の任意の直線 L はちょうど $n+1$ 個の点を含む．同様にして π の任意の点 P に対して P を含む直線はちょうど $n+1$ 個であり，これ等は，P を通らないような1直線 L 上の $n+1$ 個の各点と P とを結んで得られた直線である．

定理 20.1.1.[1] n を2以上の自然数としたとき，射影平面において次の性質 1)〜6) はすべて同値である．

1) ある1直線がちょうど $n+1$ 個の点を含む．

2) ある1点がちょうど $n+1$ 個の直線に含まれる．

3) 任意の直線はちょうど $n+1$ 個の点を含む．

4) 任意の点はちょうど $n+1$ 個の直線に含まれる．

5) 平面 π はちょうど n^2+n+1 個の点を含む．

6) 平面 π はちょうど n^2+n+1 個の直線を含む．

証：1) から 2), 3), 4) が導き出されることはすでに示した．まず1) から

---

[1] ここで与えられた自然数 n をその射影平面の位数（order）とよぶ．

5) が導かれることを示す．P_0 を π の1点とし P_0 を通る $n+1$ 個の直線を $L_1, \cdots, L_{n+1}$ とする．このとき，π の任意の点は $L_1, \cdots, L_{n+1}$ のいずれかに含まれ，各 L_i は1点 P_0 と他の n 個の点を含む．$L_1, \cdots, L_{n+1}$ のどの2つの直線に対しても，それらに同時に含まれる点は P_0 だけだから，π は $1+(n+1)n=n^2+n+1$ 個の点を含む．次に 1) から 6) が導かれることをいう．L_0 を π の1直線，L_0 に含まれる $n+1$ 個の点を $P_1, \cdots, P_{n+1}$ とする．各点 P_i は L_0 上にあり，L_0 と異なる n 個の直線に含まれる．π の直線はすべてこのようにして得られるから，π は $1+(n+1)n=n^2+n+1$ 個の直線を含む．以上により 1）から残りの 2)～6) がすべて導かれることが分かった．一方双対性により，2）から残りの 1), 3)～6) が導かれる．また 3）が 1）を，4）が 2）を導くことは自明である．次に 5）から 1）が導かれることをいう．5）により，π に含まれる点の個数は有限だから π のある直線は $m+1$ (m は整数) 個の点を持つ．このとき $m^2+m+1=n^2+n+1$, したがって $m=n$ が成り立つ．同様に 6）から 2）が導かれる．証終．

20.2. 共線変換とデザルグの定理*)

射影平面 π_1 と π_2 が**同型**であるとは，次の性質 1)～3) が満たされることをいう．

（1） π_1 の点の集合から π_2 の点の集合の上への1対1の写像 α が存在する．

（2） π_1 の直線の集合から π_2 の直線の集合の上への1対1の写像 β が存在する．

（3） π_1 の点 P_1 と直線 k_1 に対して $P_1 \in k_1$ であれば $(P_1)\alpha \in (k_1)\beta$ が成り立つ．

明らかに，写像 α, β は一方が決まれば他方も自動的に決まる．また，1直線上にある π_1 の任意の3点 P_1, Q_1, R_1 に対して，$(P_1)\alpha$, $(Q_1)\alpha$, $(R_1)\alpha$ がいつも1直線上にあるならば α は π_1 と π_2 の間の同型を定める．同様に1点

*) この節で用いられた3次元空間の性質については，Veblen-Young [1] 20-25 頁を参照．

で交わる π_1 の任意の3直線に対して，その β による像がいつも1点で交わるならば，β は同型写像を定める．平面の準同型写像とは，点と直線の間の含む含まれないという関係を保つ多対1の写像であるが，この概念はあまり役に立つとは思われない．

平面 π からそれ自身の上への同型写像を**共線変換**とよぶ．平面 π の共線変換全体は群を作る．これを平面 π の共線変換群という．

3次元空間 E_3 に埋め込まれるような平面 π_1 には，多くの種類の共線変換が存在する．π_2 を E_3 の π_1 と異なる平面とする．π_2 と π_1 の交わりとなっている直線を L とする．そこで π_1 および π_2 上にない相異なる2点 P_1, P_2 を任意に選ぶ．この時点 P_1 に対して π_1 から π_2 の上への写像（同じ記号 P_1 であらわす）を次のように定義する．すなわち π_1 の各点 Q に対して直線 P_1Q と π_2 の交点 R を対応させる．

$$Q \xrightarrow{P_1} R. \tag{20.2.1}$$

この写像 P_1 は π_1 の点の集合を π_2 の点の集合の上に1対1に写す．また，π_1 の各直線（π_1 と，点 P_1 を含むある平面 π_3 との交わりとなっている）を π_2 の直線（π_2 と π_3 の交わりとなっている）に写す．したがって P_1 が π_1 から π_2 の上への同型写像であることは明らかである．さらに，これは，直線 L（π_1 と π_2 の交わり）上の各点を固定する．同様にして点 P_2 に対して定まった π_2 から π_1 への写像 P_2

$$R \xrightarrow{P_2} S. \tag{20.2.2}$$

は π_2 から π_1 への同型写像であり L の各点を固定する．したがってこれら2つの写像をつづけてほどこしたもの

$$Q \xrightarrow{P_1} R \xrightarrow{P_2} S. \tag{20.2.3}$$

（これを α と置く）は π_1 の共線変換でありしかも L の各点を固定する．また，直線 P_1P_2 と π_1 との交点を O としたとき，

$$O \xrightarrow{P_1} T \xrightarrow{P_2} O. \tag{20.2.4}$$

(なぜならば P_1, P_2, O, T は1直線上にあるから) であるから, $(O)\alpha=O$ である. さらに k を O を通る π_1 上の任意の直線とし, Q を k に含まれる1点としたとき, (20.2.3) において, R は直線 k と直線 P_1P_2OT を含む (一意的に定まる) 平面 π_4 に含まれる. したがって (20.2.3) において S も π_4 に含まれるから S は k 上の点である. したがって α は O を通る各直線をそれ自身に移す.

一般に射影平面の共線変換 α が**中心共線変換** (配影共線変換) であるとは, 1直線 L と1点 O (L 上にあってもよい) が存在して, α は L の各点および点 O を固定し, O を通る任意の直線をそれ自身に写すことをいう. このとき直線 L を中心共線変換 α の軸, 点 O を α の中心とよぶ. 特に, O が L に含まれるとき, α を**相応** (elation) とよび, O が L に含まれないときには**ホモロジー** (homology) とよぶ. (20.2.3) で定義した α は中心共線変換である.

次に, デザルグの定理について考察する.

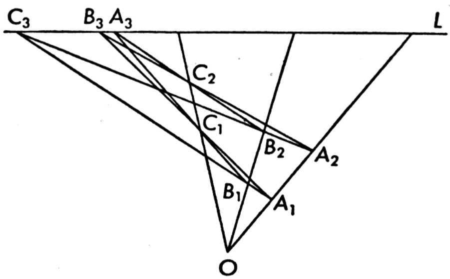


図 9. デザルグの定理

いま, 一般の射影平面において, 直線 L および相異なる三点 O, A_1, A_2 で点 A_1, A_2 は L 上になく, O, A_1, A_2 が1直線をなすものが与えられていると仮定する. このとき, 中心 O, 軸 L, $(A_1)\alpha=A_2$ なる共線変換はたかだか1つしか存在しないことを次に示す. 点 B_1 を直線 OA_1A_2 および L 上にない π の任意の点とする. 直線 A_1B_1 と L の交点を C_3 とする. $(B_1)\alpha$ は直線 OB_1 上にある. 一方, 三点 A_1, B_1, C_3 は1直線上にあるから, $(A_1)\alpha=A_2$, $(B_1)\alpha$, $(C_3)\alpha=C_3$ も1直線上にある. したがって, $(B_1)\alpha$ は OB_1 および C_3A_2 の

上にあるから，その交点（B_2 と置く）である．したがって，$(A_1)\alpha=A_2$ から，OA_1A_2 上にない任意の点 B_1 の α による像が一意的に定まった．一方，$(B_1)\alpha=B_2$ から，OA_1A_2 上の任意の点の α による像が一意的に定まる．したがって α は存在すれば一意的に定まる．

さて，C_1 を直線 OA_1A_2 および OB_1B_2 にない任意の点とする．B_1C_1 と L との交点を A_3，A_1C_1 と L との交点を B_3 とする．$(C_1)\alpha=C_2$ は A_2B_3 と OC_1 の交点である．一方，B_1, C_1, A_3 は1直線上にあるから，$(B_1)\alpha=B_2$, $(C_1)\alpha=C_2$, $(A_3)\alpha=A_3$ も1直線上にある．このようにしてできあがった図形を**デザルグの図形**とよぶ．またこの図形の存在を主張する命題を，デザルグの定理とよぶ．また，2つの三角形 A_1, B_1, C_1 と A_2, B_2, C_2 が中心 O に関して配影的であるとは，対応する各頂点を結ぶ直線がいずれも O を通ること（すなわち，OA_1A_2, OB_1B_2, OC_1C_2 が直線となること）をいう．また，2つの三角形が軸 L に関して配影的であるとは，対応する各辺の交点がいずれも L 上にあることをいう．

定理 20.2.1.（デザルグの定理）. もし2つの三角形 A_1, B_1, C_1 と A_2, B_2, C_2 が中心 O に関して配影的であれば，対応する辺，A_1B_1 と A_2B_2, A_1C_1 と A_2C_2, B_1C_1 と B_2C_2 の交点として得られる3点 C_3, B_3, A_3 は，ある1直線 L 上にある．

平面 π においてデザルグの定理が成り立つことは，π の可能なすべての中心共線変換が存在することである．このことを以下の定理で示す．

定理 20.2.2. 平面 π において，直線 L および相異なる三点 O, A_1, A_2 が与えられていて A_1, A_2 は L 上になく，OA_1A_2 が1直線をなすと仮定する．このとき，中心 O, 軸 L, $(A_1)\alpha=A_2$ なる π の中心共線変換 α はたかだか1つしか存在しない．もし π が3次元射影空間に埋め込まれれば，このような共線変換は必ず（1つ）存在する．

証：α がたかだか1つしか存在しないことはすでに示した．次に，π が3次

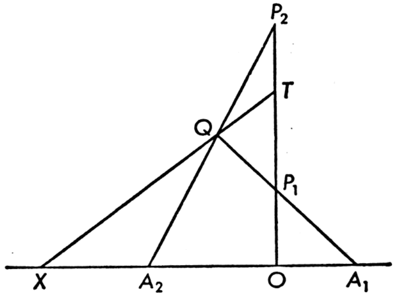


図 10. 配影共線変換

元空間 E_3 に埋め込まれていると仮定して，このような中心共線変換 α が存在することを示す．E_3 の 1 平面 π_2 を π との交わりが L となるようにとり，また π および π_2 上にない E_3 の 1 点 P_1 をとる．直線 P_1O と π_2 の交点を T とする（図10. 参照）.

直線 A_1P_1 と π_2 との交点を Q とすれば，Q は OP_1 と OA_1A_2 により定まる平面 π_3 上にある．（図10. の平面は π_3 である.）したがって，A_2Q と OP_1 は 1 点 P_2 で交わる．P_2 は π_2 上にない．なぜならば，もしそうでなければ，P_2 は T であり，A_2 は OA_1A_2 と L の交点 X と一致して A_2 は L 上にないという仮定に反するからである．同様に A_2 は O と異なるという仮定により，P_2 は π 上にない．いま，

$$\pi \xrightarrow{P_1} \pi_2 \xrightarrow{P_2} \pi$$

で，中心共線変換 α を定義すれば，軸 L，中心 O で，

$$A_1 \xrightarrow{P_1} Q \xrightarrow{P_2} A_2$$

（すなわち $A_2=(A_1)\alpha$）となる．この α が求めるものである．証終.

定理 20.2.3. 平面 α においてデザルグの定理が成り立つための必要十分条件は，π における可能なすべての中心共線変換が存在することである.

系 20.2.1. 3 次元射影空間に埋め込むことのできる任意の平面 π に対して，

デザルグの定理が成り立つ.

証：定理 20.2.2 により，定理 20.2.3 から系 20.2.1 は直ちに導かれる.

以下定理 20.2.3 を証明する.

（十分条件）π において，可能なすべての中心共線変換が存在すると仮定する．そこで2つの三角形 A_1, B_1, C_1 と A_2, B_2, C_2 が与えられていて，3直線 A_1A_2, B_1B_2, C_1C_2 がいずれも点Oを含んでいると仮定する（図9参照）．A_1B_1 と A_2B_2 の交点を C_3, A_1C_1 と A_2C_2 の交点を B_3 とする．B_3 と C_3 とを結ぶ直線をLとする．仮定により，中心 O, 軸 L, $(A_1)\alpha=A_2$ となる中心共線変換 α が存在する. 以上の構成法から分かるように, $(B_1)\alpha=B_2$, $(C_1)\alpha=C_2$ である．次に B_1C_1 と L の交点を A_3 とする．$(B_1)\alpha=B_2$, $(C_1)\alpha=C_2$, $(A_3)\alpha=A_3$ は1直線上にある．すなわち A_3 は直線 B_2C_2 上になければならない．したがって B_1C_1 と B_2C_2 の交点は A_3 に一致し，L上にある．したがってデザルグの定理が成り立つことが証明された.

（必要条件）デザルグの定理がπ において成り立つと仮定する．いま，直線Lと1直線上にある相異なる3点 O, A_1, $A_2(A_1\notin L, A_2\notin L)$ が与えられたと仮定する.（再び, 図9を参照）L上にある各点Xに対して$(X)\alpha=X$, $(O)\alpha=O$, $(A_1)\alpha=A_2$ により写像 α を定義する．もし $B_1\notin L$ かつ $B_1\notin OA_1A_2$ であれば，A_1B_1 と L の交点を C_3, A_2C_3 と OB_1 との交点を B_2 とするとき，$(B_1)\alpha=B_2$ と定義する． これによって OA_1A_2 上にないすべての点に対して α が定義された．次に上の B_1 を任意に固定しておく．このとき直線Lと3点 O, B_1, B_2 に関しても α の場合と全く同様にして写像 β を定義できる．いま，C_1 を OA_1A_2 および OB_1B_2 上にない任意の点とする．A_1C_1 とLの交点を B_3, A_2B_3 と OC_1 との交点を C_2 とする．α の定義により $C_2=(C_1)\alpha$ である．3直線 OA_1, OB_1, OC_1 はいずれも相異なるから，2つの三角形 A_1, B_1, C_1 と A_2, B_2, C_2 は中心Oに関して配影の位置にある．したがって，デザルグの定理により，対応する辺の交点は同一直線上にある．ところが点 C_3, B_3 はL上にあるから B_1C_1 と B_2C_2 の交点 A_3 も L 上にある．一方 β の定義により

$(C_1)\beta$ は B_2A_3 と OC_1 の交点である．この点は C_2 に外ならない．したがって直線 OA_1A_2 および OB_1B_2 上にない任意の点に対しては α と β が一致している．したがって直線 OA_1A_2 上では $\alpha=\beta$ と定義すれば，全平面上の点に対して α が定義された．

さて，k を O または A_1 を通らない任意の直線とする．k と L の交点を A_3，B_1 と C_1 を k 上の A_3 と異なる 2 点とする．α の定義通りに $(B_1)\alpha=B_2$，$(C_1)\alpha=C_2$ を作図する．一方定義により $(A_3)\alpha=A_3$ である．いまデザルグの定理を 2 つの三角形 A_1, B_1, C_1 と $A_2B_2C_2$ へ適用すれば，B_2, C_2, A_3 は 1 直線上にあることが分かる．このことから分かるように，もし C_1 が A_3B_1 と OA_1A_2 の交点である場合を除けば，α は直線 $k=A_3B_1$ 上の点 C_1 を直線 A_3B_2 上の点へ移す．もし $C_1=D_1$ が B_1A_3 と OA_1A_2 の交点であれば，$(B_1)\alpha=(B_1)\beta=B_2$ だから $(D_1)\beta=D_2$ は A_3B_2 と OA_1A_2 の交点である．したがって，α は k 上のすべての点を直線 A_3B_2 上の点に移す．また明らかに L 上の各点は固定され，O を通る各直線は固定される．したがってこの α が求めていた共線変換である．証終.

以上の証明から分かるように，定理 20.2.3 よりもさらに詳しい結果が成り立つ．すなわち，

定理 20.2.4. 平面 π において，中心 O，軸 L とする可能なすべての中心共線変換が存在するための必要十分条件は，O に関して配影的な 2 つの三角形で，しかも対応する辺の交点 3 個のうち 2 個が L 上にあるようなものすべてに対してだけ，デザルグの定理が成り立つ（すなわち残りの 1 個も L 上にある）ことである．

すべての平面 π が 3 次元空間に埋め込まれるわけではないので，定理 20.2.4 が限られた数の軸 L，中心 O，に対してだけしか適用できない場合がある．

20.3. 座標の導入

任意の射影平面 π に対して，一般の任置にある（すなわち，そのいずれの 3

つも同一直線上にない）4点 X, Y, O, I を選ぶ．直線 XY を**無限遠直線** L_∞ とよぶ．直線 OI を直線 $y=x$ とよぶことにする．

直線 OI 上の点Oに座標 (0,0) を与え，Iに (1,1) を，OI と XY の交点Cに1つの座標（1）を与える．OI の他の点に対しては，異なる点に対しては異なる記号bを与えるように，座標 (b,b) を与える．L_∞ 上にない点Pに対しては，XP と OI の交点が (b,b) YP と OI の交点が (a,a) であれば，座標(a,b)を与える．この規則により，OI 上の点に対しては先に定めたものと同じ座標が与えられることに注意しょう．点 (0,0) と $(1,m)$ を結ぶ直線が直線 L_∞ と点Mで交わるとき，Mに1つの座標 (m) を与えることにする．この座標 (m) は直観的には，傾きを意味すると考えられる．このようにして，Yを除く π 上の各点に対して座標が与えられたわけである．Yに対しては記号的に1つの座標 (∞) を与えることにする．

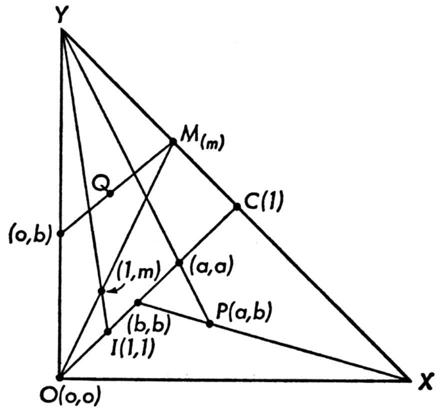


図 11. 座 標 の 導 入

次に平面における直線達を用いて，ここで定義した座標系に代数的な演算を定義する．このようにして得られる代数系のことを**三元環**(ternary ring)とよぶ．このとき，π の L_∞ と異なる各直線は，この三元環における演算を用いて表わされた方程式により定義されることが示される．たとえば，もし(x, y)が OI 上の有限な（すなわち，L_∞ 上にない）点であれば，$y=x$ が成り立ち，

逆に $y=x$ は OI を定義する方程式とみなすことができる．また，Y を通り L_∞ と異なる各直線は，その上の有限な各点 (x, y) の x 座標が一定，たとえば $x=c$ であるという性質を持ち，逆に方程式 $x=c$ はその直線を定義するとみなすことができる．

また，もし (x, y) が $C=(1)$ と $(0, b)$ を結ぶ直線上の有限の点であれば，2 項演算である加法が

$$y=x+b \tag{20.3.1}$$

で定義され，逆にこの方程式がその直線を定義するとみなすことができる．また，もし (x, y) が $O=(0, 0)$ と (m) を結ぶ直線上の有限の点であれば，2 項演算である乗法が

$$y=xm \tag{20.3.2}$$

で定義され，逆にこの方程式がその直線を定義するとみなすことができる．またさらに，点 Y を通らない 1 直線は L_∞ と 1 点 (m) で，OY と 1 点 $(0, b)$ で交わるが，もし $Q=(x, y)$ がこの直線上の点であれば，三項演算が

$$y=x\cdot m\circ b \tag{20.3.3}$$

により定義され，逆にこの方程式がその直線を定義するとみなすことができるという具合である．先に定義された加法，乗法は上の三項演算の特別な場合であると考えられ，

$$\begin{aligned} x+b&=x\cdot 1\circ b \\ xm&=x\cdot m\circ 0 \end{aligned} \tag{20.3.4}$$

が成り立つ．また，元 0, 1 に対しては，いつものように次の性質が成り立つ．

$$\begin{aligned} 0+a&=a+0=a \\ 0\,m&=m\,0=0 \\ 1\,m&=m\,1=m \end{aligned} \tag{20.3.5}$$

以下の目標は，平面 π は，その演算がある性質を満たすような三元環（ternary ring）により表現され，逆にそれ等の性質を満たす三元環は，平面を一意的に決定するということを示すことである．

定理 20.3.1. 平面 π から一般の位置にある 4 点 X, Y, O, I を選ぶことに

より，三元環 R が定まる．R には零元 0，と単位元 $1\neq 0$ が含まれ，R の三項演算 $x\cdot m\circ b$ は次の規則を満たす．

$T1$. $0\cdot m\circ c=a\cdot 0\circ c=c$

$T2$. $1\cdot m\circ 0=m\cdot 1\circ 0=m$

$T3$. 任意の a, m, c に対して，$a\cdot m\circ z=c$ となる z が一意的に存在する．

$T4$. 任意の $m_1, m_2, m_1\neq m_2, b_1, b_2$ に対して，$x\cdot m_1\circ b_1=x\cdot m_2\circ b_2$ となる x が一意的に存在する．

$T5$. 任意の $a_1, a_2, a_1\neq a_2, c_1, c_2$ に対して，$a_1\cdot m\circ b=c_1$，$a_2\cdot m\circ b=c_2$ を満たす m と b の組が一意的に存在する．

証：π から一般の位置にある4点 X, Y, O, I を選ぶことにより，すでに示したように，三項演算 $x\cdot m\circ b$ を持った三元環を作ることができた．性質 $T1$ と $T2$ が成り立つことは定義から直ちに分かる．$T3$ の主張は，(m) と (a, c) を結ぶ直線は，OY とただ一つの点 $(0, z)$ で交わるということであるから成り立つ．$T4$ の主張は，異なる傾き m_1, m_2 を持った2直線 $y=x\cdot m_1\circ b_1$ と $y=x\cdot m_2\circ b_2$ はただ一つの有限な点で交わるということであり，$T5$ の主張は，(a_1, c_1)，(a_2, c_2)，$a_1\neq a_2$ が共に有限な点であれば，これ等の2点を通り，$y=x\cdot m\circ b$ という形をした直線がただ一つ存在するということであるから $T4$. $T5$ は共に成り立つ．

逆に，$T1, \cdots, T5$ を満たす三元環 R が与えられているとしょう．まず有限の点 (a, b) と無限の点 $(m), (\infty)$ 達を作る．ここで a, b, m は R のすべての元について動く．すべての無限の点 $(m), (\infty)$ からなり，有限の点を含まない集合を無限遠直線 L_∞ とし (c, y)（c は一定）なる形の点と (∞) からなる集合を直線 $x=c$ とし，1点 (m) と $y=x\cdot m\circ b$（m, b は一定）の解である点 (x, y) からなる集合を直線 $y=x\cdot m\circ b$ と置く．このようにしてできた点と直線達の組に対して，射影平面の公理 $P1$〜$P3$ が成り立つことを示すのは容易である．しかし，幾つかの場合分けを必要とする．$(P3)$ の4点としては $(\infty), (0), (0, 0), (1, 1)$ をとればよい．$(P1), (P2)$ の詳しい証明は読者に委ね

るが，ここでは１つの場合についてだけ証明する．他の場合も同様にすればよい．２つの相異なる２直線 $y=x\cdot m\circ b_1$ と $y=x\cdot m\circ b_2$ は (m) を含み，他の無限の点を含まない．一方これらの２直線が共に有限の１点 (a,c) を含んだとすれば，$a\cdot m\circ b_1=c=a\cdot m\circ b_2$ となり $b_1\neq b_2$ であるから $T3$ に矛盾する．したがってこれ等２直線の交点はただ一つである．

20.4. Veblen-Wedderburn 系，Hall 系

この節では，ある種の共線変換群を持つ平面の性質および，そのような平面の三元環の性質について調べる．

補題 20.4.1. 射影平面 π の相異なる２直線上の各点を固定する共線変換は恒等写像である．

証：共線変換 α が１点 Q で交わる相異なる２直線 L_1, L_2 上の各点を固定したとする．P を L_1, L_2 上にない任意の点とし，L_1 上の Q と異なる２点 R, S を任意に選ぶ．PR と L_2 の交点を T，PS と L_2 の交点を U とする．R, S, T, U はいずれも α で固定されるから，直線 RT, SU はいずれも α で固定される．したがってその交点 P も固定される．仮定により，L_1, L_2 の点は α により固定されていたから，平面の各元は α により固定される．したがって α は恒等変換である．

補題 20.4.2. 射影平面のある１直線上の各点と，その直線上にない２点をそれぞれ固定する共線変換は恒等変換である．

証：共線変換 α が直線 L の各元と，L 上にない２点 P_1, P_2 を固定したとする．P を直線 L および，直線 P_1P_2 上にない任意の点とし，P_1P と L の交点を Q_1，P_2P と L の交点を Q_2 とする．P は L 上の点でも P_1P_2 上の点でもないから，直線 P_1PQ_1 と P_2PQ_2 は相異なる．したがって P_1, Q_1, P_2, Q_2 は相異なり，それぞれ α により固定されるから，直線 P_1Q_1 と P_2Q_2 は α で固定され，したがってその交点 P も α で固定される．α は，L 上の各点と，P_1P_2

上にない各元をすべて固定するから，α はまた，L上の各点と，P_1 を通り P_1P_2 と異なる1つの直線，たとえば P_1Q_1，上の各点を固定する．したがって補題20.4.1により，α は恒等変換である．証終．

以上のことから分かるように，恒等変換と異なる共線変換が1つの直線L上の各点を固定するならば，その共線変換によって固定されるL上にない点の個数は高々1つである．

定理 20.4.1. 直線 L上の各点を固定する共線変換 α に対して，平面の1点Cが存在して，Cは α により固定され，また，Cを通るすべての直線が α により固定される．さらに，α が恒等変換でなければ，α はそれら（直線 L，L上の各点，点C，点Cを通る各直線）以外の点，直線を固定しない．双対的に，共線変換 α が1点Cと，Cを通る各直線を固定すれば，直線Lが存在して，α はL上の各点を固定する．さらに α が恒等変換でなければ，α はそれら以外の点，直線を固定しない．

証：平面 π の共線変換 $\alpha\neq 1$ が L上の各点を固定したとする．補題20.4.2により，α はたかだか1つのL上にない点を固定する．まず，α がL上にない点Cを固定したと仮定する．Cを通る1つの直線が L と $Q(\neq C)$ で交わるとすれば，C, Q は共に α で固定されるから，直線 CQ も α で固定される．したがってCを通る各直線は α により固定される．もし L と異なり，点Cを通らないある直線 L_2 が α により固定されたとすれば，L_2 の各点は α により固定される．なぜならば，その点は，その点とCとを結ぶ直線の L_2 との交点であり，しかもいづれの直線も α によって固定されるからである．したがって補題20.4.1により α は恒等変換でなければならない．また，補題20.4.2により，α により固定される点はCとL上の各点だけである．

次に α が L 上にない点はどれも固定しないと仮定する．Pを L 上にない任意の点とするとき，α によるPの像 $P\alpha$ はPと異なり，またL上にない．したがって，直線 $M=PP\alpha$ の Lとの交点CはPとも $P\alpha$ とも異なる．したがって $M=PC$ であり，$M\alpha=P\alpha C\alpha=P\alpha C$ であるから $M=M\alpha$ である．した

がって，L上にない任意の点Pはαにより固定されるある1つの直線M上にある．またPを含み，αにより固定される直線はただ一つである．なぜならば，もしそうでないならば，点Pもαにより固定されることになり仮定に反するからである．さて，αが直線$M=PC$を固定したとし，L上およびM上にない点Qを任意にとってくる．Qを通りαにより固定される直線（ただ一つ存在する）をNとする．MとNはαによりそれぞれ固定されるからL上の点すなわちCで交わる．したがってαにより固定される直線はすべてCを通ることが証明された．一方，Cを通り，Lと異なる任意の直線Kは，L上にない1点Rを含む．このとき点Rを通り，αにより固定される直線がただ一つだけ存在したが，これはCを通らなければならないので，Kに他ならない．したがって，Cを通る任意の直線がαにより固定されることが分かった．もしαにより直線L，L上の各点，点CおよびCを通る各直線以外の点や直線が固定されれば，補題 20.4.1 および 20.4.2 によりαは恒等変換である．

定理の後半は，双対性により得られる．証終．

したがって，この定理における共線変換は§20.2 で見た**中心共線変換**である．中心Cと軸LをはっきりさせるためにC-L-**共線変換**とよぶこともある．§20.2 と同様に中心Cが軸L上にあるときは**相応**（elation），CがL上にないときは**ホモロジー**（homology）とよぶ．

補題 20.4.3. 中心共線変換αは，中心C，軸L，L上にない任意の1点$P(\neq C)$のαによる像$P\alpha$により完全に定まる．P, $P\alpha$, Cは1直線上にある．

証：共線変換α_1, α_2が共に，中心C，軸Lを持ち，$P\alpha_1=P\alpha_2$とする．このとき$\alpha_1\alpha_2^{-1}$もLを軸とし，中心がCであり，さらに点Pを固定する．したがって，定理 20.4.1 により，$\alpha_1\alpha_2^{-1}=1$，したがって$\alpha_1=\alpha_2$となる．証終．

定理 20.4.2. 中心がそれぞれC_1, C_2, $C_1\neq C_2$，軸が共にLである2つの相応の積は，中心が$C_3\neq C_1$, C_2，軸がLの相応である．

証：α_1 は中心 C_1，軸 L を持つ相応，α_2 は中心 $C_2 \neq C_1$，軸 L を持つ相応とする．$\alpha_1\alpha_2$ は L の各点を固定する共線変換である．したがって，定理 20.4.1 により $\alpha_1\alpha_2=\alpha_3$ は L を軸とする中心共線変換である．α_3 が相応であることを示すためには，L 上にないどの点も α_3 により固定されないことを示せばよい．P を L 上にない点とするとき，$P\alpha_3=P$ であれば，$P\alpha_1=P\alpha_2{}^{-1}$ である．一方，C_1, P, $P\alpha_1$ は，1直線上にある．また C_2, P, $P\alpha_2{}^{-1}$ も1直線上にある．したがって，これらの2直線は一致する．それゆえ，それぞれの直線の L との交点も一致する．すなわち $C_1=C_2$ となる．これは仮定に反する．したがって，$\alpha_3=\alpha_1\alpha_2$ は L 上にない，いかなる点も固定しないから，α_3 は L を軸とする相応である．相応 α_3 の中心 C_3 は C_1 と異なる．なぜならば，もし $C_3=C_1$ ならば，$\alpha_2=\alpha_1{}^{-1}\alpha_3$ は，中心が C_1 の相応となり，仮定に反するからである．同様に $C_3 \neq C_2$ である．証終．

C–L–中心共線変換全体の作る群 $G=G(C, L)$ を考えよう．もし，$P \neq C$, $P \notin L$ であれば，各 $\alpha \in G$ に対して，C, P, $P\alpha$ は1直線上にある．もし，CP の各点 $Q \neq C$, $Q \notin L$ に対して $P\alpha=Q$ となる $\alpha \in G$ が存在するならば，π を **C–L–可移**とよぶことにする．このことは可能な C–L–共線変換がすべて実際に存在するということである．言い換えれば，π が C–L–可移であるということは，C を通るある直線 $M \neq L$ に対して，C および M と L の交点を除いた M の各点が C–L–共線変換により相互に移り得るということを意味する．これは，C を通る任意の直線 $M \neq L$ に対して成り立っている．

定理 20.4.2 により，軸が L であるような相応全体は群 $G(L)$ を作る．この群 $G(L)$ を，軸 L に関する**移行群**（translation group）とよぶ．

定理 20.4.3.（**Baer** [10]） 直線 L 上の相異なる2点 C_1, C_2 に対して，中心がそれぞれ C_1, C_2, $C_1 \neq C_2$, 軸が共に L である2つの相応群 $G(C_1, L)$, $G(C_2, L)$ が共に単位群でなければ，軸 L に関する移行群 $G(L)$ はアーベル群である．このとき，$G(L)$ の単位元と異なる各元の位数は，（1）すべて無限であるか，または（2）すべて素数 p であるか，のいずれかである．

証：$\alpha_1 \in G(C_1, L)$, $\alpha_1 \neq 1$, $\alpha_2 \in G(C_2, L)$, $\alpha_2 \neq 1$ とする．P を L 上にない任意の点とする．このとき次の直線が得られる．

$$L_1 : C_1,\ P,\ P\alpha_1,$$
$$L_2 : C_2,\ P,\ P\alpha_2,$$
$$L_1\alpha_2 : C_1,\ P\alpha_2,\ P(\alpha_1\alpha_2)$$
$$L_2\alpha_1 : C_2,\ P\alpha_1,\ P(\alpha_2\alpha_1).$$

一方，C_2, $P\alpha_1$, $(P\alpha_1)\alpha_2 = P(\alpha_1\alpha_2)$ は1直線上にあり，C_1, $P\alpha_2$, $(P\alpha_2)\alpha_1 = P(\alpha_2\alpha_1)$ も1直線上にある．したがって，$P(\alpha_1\alpha_2) = P(\alpha_2\alpha_1)$ が各 $P \notin L$ に対して成り立つ．ゆえに，$\alpha_1\alpha_2 = \alpha_2\alpha_1$ である．したがって，$\alpha_1 \in G(C_1, L)$ は $C_2 \neq C_1$ なる任意の $G(C_2, L)$ の各元 α_2 と可換である．次に，$\beta_1 \neq 1$ が $G(C_1, L)$ の α と異なる元であれば，$\beta_1\alpha_2$ は中心が $C_3 \neq C_1$, C_2 の相応である．したがって α_1 は $\beta_1\alpha_2$ と可換であり，また，α_1 は α_2 と可換であるから，α_1 と β_1 は可換である．したがって，$G(L)$ はアーベル群であることが証明された．一般に，$G(C_1, L)$ は，他のすべての $G(C_i, L)$, $C_i \in L$ が単位元のみからなるときには，アーベル群になるとは限らない．

次に，もし $G(L)$ の各元の位数が無限ならば（1）が成り立つ．そこで $G(L)$ が，位数有限の元を含むとする．そうすれば $G(L)$ は位数が素数の元を含む．それを $\alpha_1 \in G(C_1, L)$, $C_1 \in L$, $\alpha_1{}^p = 1$（p は素数）とする．任意の $\alpha_2 \in G(C_2, L)$, $\alpha_2 \neq 1$, $C_2 \in L$, $C_2 \neq C_1$ に対して，$\alpha_1\alpha_2 = \alpha_3 \in G(C_3 L)$, $C_3 \neq C_1$, C_2, となる $C_3 \in L$ が存在する．このとき，$(\alpha_1\alpha_2)^p = \alpha_2{}^p = \alpha_3{}^p$ は $G(C_2, L)$, $G(C_3, L)$ に共通な元だから単位元である．したがって $\alpha_2{}^p = 1$ が得られる．このことから同様にして，各 $\beta_1 \in G(C_1, L)$ に対して，$\beta_1{}^p = 1$ が得られる．したがって，$G(L)$ の単位元と異なる元の位数はすべて p である．証終．

定理 20.4.4. 平面 π が，L 上の相異なる2点 C_1, C_2 に対して，C_1-L-可移かつ C_2-L-可移であれば，π は各 $C \in L$ に対して，C-L-可移である．

証：点 $C \neq C_1$, C_2 を通る L と異なる直線 M を一つ選び，M 上の点で C と異なる2点 P, Q を任意に選ぶ．直線 PC_1 と QC_2 の交点を S とする．C_1-L

および C_2-L-可移性から, $\alpha_1 \in G(C_1, L)$, $P\alpha_1 = S$, $\alpha_2 \in G(C_2, L)$, $S\alpha_2 = Q$ なる α_1, α_2 が存在する．このとき，$\alpha_1\alpha_2 = \alpha_3$ は軸 L に関する相応であり，3点 P, $P\alpha_3 = Q$, C は1直線上にある．したがって，$\alpha_3 \in G(C, L)$ であり，π は C-L-可移である．証終．

系 20.4.1. 直線 L 上の相異なる2点 C_1, C_2 に対して平面 π が，C_1-L-可移かつ C_2-L-可移であるならば $G(L)$ は中心が L 上にあるすべての可能な相応を含む．π が各 $C \in L$ に対して C-L-可移であるとき，π は軸 L に関する移行平面とよぶことにする．

相応の性質は，平面 π に座標を定める三元環の性質にどう反映するかということを考える．初めに π が C-L-可移である場合を考える．相応の軸 L を無限遠直線 L_∞ として，中心 C を $Y = (\infty)$ として考えよう．

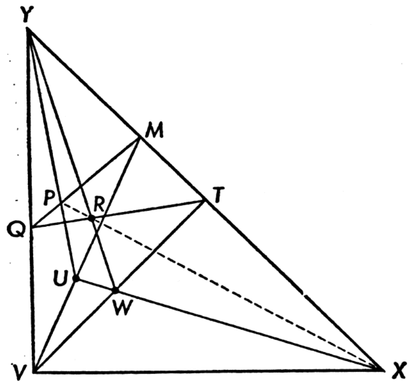


図 12. 線 型 性 定 理

定理 20.4.5. 平面が Y-L_∞ 可移であるための必要十分条件は，対応する三元環において次の性質 1), 2) が共に成り立つことである．

1) $a \cdot m \circ b = am + b$

2) 加法に関して群を作る．

証：π が Y-L_∞ 可移であると仮定する．図12において，$V = (0, 0)$, $Q = (0,$

b)，$X=(0)$，$T=(1)$，$M=(m)$ とすると，直線 YQV は直線 $x=0$ で表わされる．このとき，直線 MQ は $y=x\cdot m\circ b$ で表わされる．MQ 上に $P=(a, a\cdot m\circ b)$ なる点をとり，直線 VM（すなわち $y=xm$），直線 TQ（すなわち $y=x+b$），直線 YP（すなわち $x=a$）を引く．U は YP と VM の交点であるから $U=(a, am)$ である．次に直線 UX（すなわち $y=am$）を引く．UX は，$VT(y=x)$ と点 $W=(am, am)$ で交わる．したがって，$YW(x=am)$ と $QT(y=x+b)$ は $R=(am, am+b)$ で交わる．もし，3点 P, R, X が同一直線上にあれば，RX は $y=am+b$ で表わされ，かつ $P=(a, a\cdot m\circ b)$ であるから，$a\cdot m\circ b=am+b$ が成り立つ．次に P, R, X が同一直線上にあることを示す．仮定により，π は Y-L_∞ 可移であるから，L_∞ の各点および Y を通る各直線を固定し，$V\beta=Q$ すなわち $(0,0)\beta=(0,b)$ を満たす Y-L_∞ 共線変換 β が存在する．したがって，β は直線 $YPU(x=a)$ および $YRW(x=am)$ を固定する．また $(VM)\beta=QM$，$(VT)\beta=QT$ である．したがって $U\beta=P$，$W\beta=R$ が成立する．また，もちろん $X\beta=X$ である．一方，U，W, X は同一直線 $y=am$ 上にあるから，$U\beta, W\beta, X\beta$，すなわち P, R, X も同一直線 $y=am+b$ 上にある．したがって $P=(a, am+b)$，$a\cdot m\circ b=am+b$ であり，1）は証明された．

$(0,0)\beta=(0,b)$ で定まった共線変換 β が一般の点 (a,c) にどう働くかを次に考察しよう．容易に分かるように

$$y=x \longrightarrow y=x+b$$
$$x=c \longrightarrow x=c$$
$$(c,c) \longrightarrow (c,c+b)$$
$$y=c \longrightarrow y=c+b$$
$$x=a \longrightarrow x=a$$
$$(a,c) \longrightarrow (a,c+b)$$

したがって，一般に，δ が $(0,0)\delta=(0,d)$ で決まる Y-L_∞-共線変換であれば，$(u,v)\delta=(u,v+d)$ が成り立つ．したがって，

$$(0,0)(\beta\delta)=[(0,0)\beta]\delta=(0,b)\delta=(0,b+d)$$

であり，一般に $(a,c)(\beta\delta)=[a, c+(b+d)]$ である．一方，$[(a,c)\beta]\delta=(a, c+b)\delta=[a,(c+b)+d]$ であるから，加法は結合律

$$c+(b+d)=(c+b)+d$$

を満たす．したがって平面における加法は，ループであり，また零元を持つから，群を作る．よって 2) は証明された．

逆に，性質 1), 2) を満たす，平面 π の三元環が与えられているとする．各 $b\in R$ に対して，写像 $\beta=\beta(b)$ を次のように定める．π の点達に対して

$$(\infty) \longrightarrow (\infty)$$

$$(m) \longrightarrow (m)$$

$$(a,c) \longrightarrow (a, c+b)$$

π の直線達に対して，

$$L_\infty \longrightarrow L_\infty$$

$$x=a \longrightarrow x=a$$

$$y=xm+t \longrightarrow y=xm+(t+b).$$

この写像 β は共線変換である．なぜならば，もし (a,c) が $y=xm+t$ 上にあれば，$c=am+t$，したがって

$$c+b=(am+t)+b=am+(t+b)$$

であり，$(a, c+b)$ は $y=xm+(t+b)$ 上にある．また，β が共線変換であることをいうための他の条件も容易に証明される．したがって，β は $(0,0)$ を $(0,b)$ に移す Y-L_∞ 共線変換であるが，b は任意に選んでよいから，π は Y-L_∞ 可移である．証終．

移行平面に対して，上の定理に対応するものは次の定理である．

定理 20.4.6. 平面 π が軸 L_∞ に関する移行平面であるための必要十分条件は，対応する三元環が Veblen-Wedderburn 系となることである．すなわち次の 1)〜5) の性質が成り立つことである．

1)　加法はアーベル群を作る．

2)　乗法は（零元 0 を除いて）ループを作る．

3) $(a+b)m=am+bm$

4) $r\neq s$ ならば $xr=xs+t$ は唯一の解 x を持つ.

5) $a\cdot m\circ b=am+b$

証：定理 20.4.4 により π が軸 L_∞ に関する移行平面であるための必要十分条件は, π が Y-L_∞-可移かつ X-L_∞-可移であることである. もし π が軸 L_∞ に関する移行平面ならば, 定理 20.4.5 により, 5) の $a\cdot m\circ b=am+b$ は成り立ち, また加法は群を作る. 定理 20.4.5 の証明の中で示したように, 各元 $b\in R$ に対して, 各点 (a,c) を $(a,c+b)$ に移す写像 $\beta(b)$ が存在する. 一方, 定理 20.4.3 により移行群はアーベル群だから, $\beta(b)\beta(d)=\beta(d)\beta(b)$ が成り立ち, したがって, $(a,c+b+d)=(a,c+d+b)$ したがって, $b+d=d+b$ が成り立ち, Rにおける加法はアーベル群である. したがって 1) は証明された.

次に, 任意の元 $b\in R$ に対して, $(0,0)$ を $(b,0)$ に移す X-L_∞-共線変換 (相応) をとれば

$$
\begin{aligned}
(0,0) &\longrightarrow (b,0)\\
y=x &\longrightarrow y=x-b\\
y=a &\longrightarrow y=a\\
(a,a) &\longrightarrow (a+b,a)\\
x=a &\longrightarrow x=a+b\\
y=am &\longrightarrow y=am\\
(a,am) &\longrightarrow (a+b,am)
\end{aligned}
$$

が成り立つ. また, $(0,0)\rightarrow(b,0)$ だから,

$$y=xm \longrightarrow y=xm-bm$$

が成り立つ. 一方 (a,am) は $y=xm$ 上にあるから, $(a+b,am)$ は $y=xm-bm$ 上にあり, したがって

$$am=(a+b)m-bm$$

したがって, $am+bm=(a+b)m$ が成り立ち, 分配律 3) が証明された.

平面からできる三元環の乗法は常にループを作るから，2）は成り立つ．4）の主張は，もし $r \neq s$ ならば直線 $y=xr$ と $y=xs+t$ は一点で交わるということであるから，4）も成り立つ．証終．

性質 1), 2), 3), 4）を満足する加法と乗法という2つの二項演算が定義された元の集合を **Veblen-Wedderburn 系**（Veblen-Wedderburn system）とよぶ．この名称は，これが彼等の論文〔1〕ではじめて取り扱われたことに由来する．

逆に，任意の Veblen-Wedderburn 系は，軸 L_∞ を持ったある移行平面の座標系として用いられることを，次に示そう．まず平面の点として，1）有限の点(a, b)，ここで a, b はRの元すべてにわたる．2）無限の点 (m)，ここで m はRの元すべてにわたる．3) $Y=(\infty)$ をとり，直線として，1）点 (∞)と(m) 達からなる直線 L_∞. 2）点 (∞) と (c, d) 達（d はRの元すべてにわたる）からなる直線 $x=c$. 3)点 (m) と $(a, am+b)$ $(a, b$ はRの示すべてにわたる）達からなる直線 $y=xm+b$ をとる．このとき，相異なる2点を通る直線がただ一つ存在すること，相異なる2直線はただ一点で交わること，および4点$(0, 0)$, $(1, 1)$, (∞), (0) はどの3つも同一直線上にないことは直ちに示される．この証明においては，いくつかの場合わけが必要とされるが，性質 4）は2直線 $y=xr+b$, $y=xs+c$, $r \neq s$は一点で交わることを示すのに用いられる．

Veblen-Wedderburn 平面において，各点に対しては

$$(x, y) \longrightarrow (x+r, y+s)$$
$$(m) \longrightarrow (m)$$
$$(\infty) \longrightarrow (\infty)$$

各直線に対しては

$$x=c \longrightarrow x=r+c$$
$$y=xm+b \longrightarrow y=xm-rm+s+b$$

で定義された写像がすべての r, s について，共線変換であることは容易に示せる．もし $s=rt$ であれば，この共線変換は軸 L_∞，中心 (t) の相応である．したがって Veblen-Wedderburn 平面は，軸 L_∞ に関する移行平面である．

任意の結合的な可逆環 (division ring) はもちろん, Veblen-Wedderburn 系であり, さらに結合的でない可逆環も, Veblen-Wedderburn 系である. 乗法が結合的な Veblen-Wedderburn 系は, **擬体** (near-field) とよばれる. これについてはまた先で触れる. 先にいって (§20.9 で) 示すが, 同型でない Veblen-Wedderburn 系が同一の平面の座標系になる場合もある. なぜかといえば, π が L_∞ を軸とする移行平面であるとき, X と Y を入れ換えると, また新しく三元環ができる. これは定理 2.4.6 によりやはり Veblen-Wedderburn 系になるが, 一般にもとのものと同型とは限らないからである.

Hall 系とよばれる Veblen-Wedderburn 系の1つのクラスを次に構成しょう. Hall [2] 参照.

定理 20.4.7. 体 F と F 上の既約な二次多項式 $f(x)=x^2-rx+s$ が与えられているとする. このとき, $a+ub$, a, $b\in F$ なる形の元の集合 J は次に定める演算 1), 2), 3) により, Veblen-Wedderburn 系を作る.

1) $(a_1+ub_1)+(a_2+ub_2)=(a_1+a_2)+u(b_1+b_2)$

2) $c\in F$ に対して $(a+ub)c=ac+u(bc)$

3) $z=a+ub$, a, $b\in F$, $b\neq 0$ と $w=c+zd$, c, $d\in F$ に対して,

$$\begin{aligned} wz&=ds+z(c+dr)\\ &=ac+adr+ds+u(bc+bdr) \end{aligned}$$

さらに, J は分配律 $(x+y)z=xz+yz$ を満たし, $c\in F$ に対して $cx=xc$, $c(xy)=(cx)y=(xc)y$ が成り立つ. さらに $z\notin F$ なる任意の元は方程式 $z^2-rz-s=0$ を満たす.

証：上の定義により, 加法は意味を持ち, 明らかに, アーベル群を作る. また乗法も意味を持つが, 積 xy に対して, (2) の $y=c\in F$ の場合と (3) の $y=z\in F$ の場合の本質的に異なった2通りの演算があることに注意しよう. 分配則 $(x+y)z=xz+yz$ は成り立つ. なぜならば, $z\in F$, $z\notin F$ に従い (2), (3) を用いて直接に計算してやればよい.

もし $z\notin F$ ならば, (3) により, $z^2=rz+s$ が成り立つ. また, $c\in F$ に対し

て，（3）により $cz=zc$ が成り立つ．c, $x\in F$ に対しては明らかに $cx=xc$ である．F の単元1はまた J の単元になる．次に乗法がループを作ることを示すために $xy=v$ ($x\neq 0, y\neq 0, v\neq 0$) において，$x$, y, v のどの2つも残りの1つを一意的に決定することを示す．x, y は $xy=v$ を一意的に決定する．なぜならば $y\in F$, $y\notin F$ に従い，（2），（3）によって決まるからである．また，$x\neq 0$, $y\neq 0$ ならば $v\neq 0$ である．なぜならば，$y\in F$ の場合は（2）から明らかであり，$y\notin F$ の場合は $y=a+ub$, a, $b\in F$, $b\neq 0$ と書けるから $s\neq 0$ であることを用いれば（3）により $v\neq 0$ が得られるからである．次に，$y\neq 0$, $v\neq 0$ が与えられたときには，（2），（3）を場合によって使いわけることによって，$xy=v$ を満たす $x\neq 0$ がただ一つ存在することが分かる．

さて，$x\neq 0$ と $v\neq 0$ が与えられた場合は，もう少し複雑である．このとき $x=a+ub$, $v=c+ud$, $a, b, c, d\in F$ と書かれているが，もし $ad-bc=0$ ならば $af=c$, $bf=d$ なる F の元 $f(\neq 0)$ が一意的に存在し，この f に対して $xf=v$ が成り立つ．すなわち，この f は上の関係を満たす唯一の J の元である．そこで，$ad-bc\neq 0$ と仮定する．$y=y_1+uy_2$, y_1, $y_2\in F$, $y_2\neq 0$ なる J の元を取ってくれば，$x=(a-by_1y_1^{-1})+y(by_2^{-1})$, $xy=sby_2^{-1}+y(a-by_1y_2^{-1}+rby_2^{-1})$ および，$v=(c-dy_1y_2^{-1})+y(dy_2^{-1})$ と表わすことができる．したがって，$xy=v$ なる関係から次の式が得られる．

$$ay_2-by_1=d-rb$$

$$cy_2-dy_1=sb$$

$ad-dc\neq 0$ であるから，y_1, y_2 に関するこれらの方程式は，一意的な解を持つ．しかも $y_2=(d^2-rbd-sb^2)/(ad-bc)$ となる．ここで $y_2\neq 0$ である．なぜならば x^2-rx-s は F 上既約であるから，$d=0$, $b=0$ のとき以外は $d^2-rbd-sb^2$ は零にならないからである．この解 y_1, y_2 に対する $y\notin F$ が $xy=v$ を満たす J の元である．以上によって，J は零元をのぞいて乗法に関してループを作ることが証明された．

次に，m, $n\in J$, $m\neq n$ に対して $xm=xn+v$ が，ただ一つだけ解を持つことを示す．もし，2つの解 x_1, x_2, $x_1\neq x_2$ が存在したとすると $(x_1-x_2)m$

$=(x_1-x_2)n$ となり J が乗法に関してループとなっていることに反する．したがって解は存在すれば一意的に定まる．次に解が存在することを示す．m, n がともに F の元であれば，解が存在することは容易に分かる．そこで，$m \notin F$ と仮定する（もし $m \in F$, $n \notin F$ であれば $xn=xm-v$ について考えればよい）．このとき n, v を m を使って表わせる．まず，$n=c \in F$, $v=v_1+mv_2$, $v_1, v_2 \in F$ の場合を考える．$x=x_1+mx_2$ と置けば $xm=xn+v$ なる関係から，

$$-cx_1+sx_2=v_1,$$
$$x_1+(r-c)x_2=v_2,$$

が得られる．一方 x^2-rx-s は F 上既約であるから，この連立方程式の係数行列の行列式 c^2-rc-s は零でない．したがって解が一意的に存在する．次に $n=a+mb$, $(b \neq 0)$ $v=v_1+mv_2$ の場合を考える．$x=x_1+mx_2$ と置けば，

$$ax_1+(a^2b^{-1}-ab^{-1}r-b^{-1}s+s)x_2=v_1$$
$$(1-b)x_1+ax_2=v_2$$

が得られる．この係数行列の行列式は $-b^{-1}[a^2-ra(1-b)-s(1-b)^2]$ であり，$b \neq 0$ かつ x^2-rx-s が既約であることから零ではない．したがってこの方程式の解は一意的に存在する．以上のことから，J が Veblen-Wedderburn 系であることが証明された．証終.

20.5. Moufang 平面とデザルグ平面

前節では，平面が Veblen-Wedderburn 系で座標づけられるためには，その平面が直線 L_∞ に関して移行平面であることが必要かつ十分であることを示した．もし平面が，2つ以上の直線に関して移行平面であれば，その平面および座標系はどのようになるだろうか？　この節では，この問に対する答を与える．

定理 20.5.1. 平面 π が相異なる2直線に関して移行平面であれば，π はその2直線の交点 Q を通る任意の直線に関して移行平面である.

系 20.5.1. π が一点で交わらない3直線に関して移行平面であれば，π は任

意の直線に関して移行平面である.

証：直ちに分かるように，系 20.5.1 は定理 20.5.1 から導かれる.

以下定理 20.5.1 の証明を行なう.

一点Yで交わる 2 直線 L_1, L_2 が与えられていて，π は L_1 および L_2 に関して移行平面であると仮定する．Yを通る任意の直線をL_3とし，CをL_3上のYと異なる任意の点とする．Cを通り L_3 と異なる直線 L を引き，L_1 との交点を R, L_2 との交点をSとする．このとき，軸L_1, 中心RでSをCへ，したがってL_2 を L_3 へ写すような相応 α が存在する．L 上の C と異なる任意の 2 点をU, Vとする．このとき，$U\alpha \in L$, $V\alpha \in L$ かつ π は L_2 に関して移行平面であるから中心S，軸 L_2 かつ $(U\alpha)\beta = V\alpha$ を満たす相応 β が存在する．このとき $\alpha\beta\alpha^{-1}$ は L_3 の各点および直線Lを固定しL上にはC以外に固定点を持たずかつ点Uを点Vに写す．したがって定理 20.4.1 により，$\alpha\beta\alpha^{-1}$ は中心C，軸 L_3 の相応である．すなわち π においてCを中心とし，L_3 を軸とする，すべての可能な相応が存在することが分かった．いまCは L_3 上のYと異なる任意の点としてよかったから，系 20.4.1 により，π は軸 L_3 に関する移行平面である．証終.

定理 20.5.2. 平面 π が点 $Y=(\infty)$ を通るすべての直線に関して移行平面であるための必要十分条件は，次の 1)，2) が同時に満たされることである.

1)　有限直線はすべて一次方程式 $x=c$ および $y=xm+b$ により与えられる．(線型条件)

2)　π を座標づける 3 元環Rは Veblen-Wedderburn 系であり，次の条件を満たす.

2.1)　加法はアーベル群である.

2.2)　$(a+b)m=am+bm$

2.3)　$a(s+t)=as+at$

2.4)　各 $a\neq 0$ は $aa^{-1}=1=a^{-1}a$ となる逆元 a^{-1} を持つ.

2.5)　$a^{-1}(ab)=b$

証：(必要条件) π は $Y=(\infty)$ を通る任意の直線に関して移行平面であると仮定する．このとき，もちろん π は L_∞ に関しても移行平面であるから定理 20.4.6によって，(1) は成り立ち，Rは Veblen-Wedderburn 系である．したがって 2.1)，2.2) も明らかである．

$Y=(\infty)$ を中心 $x=0$ を軸とし (0) を (m) へ移すような相応を考えれば，

$$(0) \longrightarrow (m)$$
$$(0,b) \longrightarrow (0,b)$$
$$y=b \longrightarrow y=xm+b$$
$$x=a \longrightarrow x=a$$
$$(a,b) \longrightarrow (a,am+b)$$

である．特に

$$(1,t) \longrightarrow (1,m+t)$$
$$(0,0) \longrightarrow (0,0)$$

であるから

$$y=xt \longrightarrow y=x(m+t)$$

である．一方

$$(a,at) \longrightarrow (a,am+at)$$

であり，(a,at) は $y=xt$ 上にあるから $(a,am+at)$ は $y=x(m+t)$ 上にある．したがって $am+at=a(m+t)$ であり，左分配律 2.3) が成り立つ．

次に，中心 (0,0)，軸 $x=0$ とし (0) を $(-1-a,0)$ に写す相応を考えれば

$$(0) \longrightarrow (-1-a,0)$$
$$(0,1+a) \longrightarrow (0,1+a)$$

であるから，

$$y=1+a \longrightarrow y=x+1+a$$

また

$$(0) \longrightarrow (-1-a,0)$$
$$(0,b+ab) \longrightarrow (0,b+ab)$$

であるから，

$$y=b+ab \longrightarrow y=xb+b+ab$$

である．また

$$y=1+a \longrightarrow y=x+1+a.$$

$$y=x(1+a) \longrightarrow y=x(1+a)$$

であるから，$a\neq 0$ ならば適当な d が存在して，

$$(1, 1+a) \longrightarrow (d, d+1+a),$$

したがって $d(1+a)=d+1+a$ が成り立つ．

また，

$$(\infty) \longrightarrow (\infty)$$

$$(1, 1+a) \longrightarrow (d, d+1+a)$$

であるから，

$$x=1 \longrightarrow x=d$$

である．

さらに，

$$y=x(b+ab) \longrightarrow y=x(b+ab)$$

$$y=b+ab \longrightarrow y=xb+b+ab$$

であり

$$(1, b+ab) \longrightarrow (d, d[b+ab]),$$

したがって

$$d(b+ab)=db+b+ab$$

が成り立つ．

いま，$a\neq 0$ かつ $(-1-a, 0)\neq(0, 0)$（すなわち $a\neq -1$）と仮定する．上に示したように，このaに対して $d(1+a)=d+1+a$ を満たす d が存在する．しかもそのとき，任意の b に対して，$d(b+ab)=db+b+ab$ が満たされる．ここで $d=u+1$ と置き，分配律を用いれば，

$$ua=1$$

および

$$u(ab)=b$$

を得る．また分配律を用いて直接計算すれば分かるようにこの式は $a=-1$ に対しても $u=-1$ と置くことにより成り立つ．$u\neq 0$ であるから，

$$vu=1$$

かつ

$$v(ua)=a$$

を満たす v が存在する．このとき $v=a$ である．したがって，$u=a^{-1}$ と置けば，$aa^{-1}=a^{-1}a=1$ かつ $a^{-1}(ab)=b$ であるから，(2.4)，(2.5) は示された．

（十分条件）平面 π の座標環 R に対して，条件（1），（2）が成り立つと仮定する．定理 20.4.6 により，π は直線 L_∞ に関して移行平面である．したがって以下，定理 20.5.1 から分かるように，L_∞ を Y を通るある直線に移すような π の共線変換が存在することを示しさえすれば良い．ところで，

$$(\infty)\longrightarrow(\infty)$$
$$(m)\longrightarrow(1,m)$$
$$(-1,m)\longrightarrow(-m)$$
$$(0,b)\longrightarrow(0,b)$$
$$(c,d)\longrightarrow[(1+c^{-1})^{-1},(1+c)^{-1}d],\quad c\neq 0,-1$$
$$L_\infty\longrightarrow x=1$$
$$x=-1\longrightarrow L_\infty$$
$$x=0\longrightarrow x=0$$
$$x=c\longrightarrow x=(1+c^{-1})^{-1},\quad c\neq 0,-1$$
$$y=xm+b\longrightarrow y=x(m-b)+b$$

で定めた写像は求めている共線変換となる．以下これを示す．まず，この写像により点と直線の間の含む含まれないの関係が保たれることを示す．そのために，もし (c,d) が $y=xm+b$ の上にあれば，その点の像もその直線の像上にあることを示す．したがって

$$(1+c)^{-1}(cm+b)=(1+c^{-1})^{-1}(m-b)+b$$

が恒等式であることを示せばよいが，これには規則 1)，2) を用いて

$$(1+c)^{-1}(cm)=(1+c^{-1})^{-1}m$$

$$(1+c)^{-1}b=(1+c^{-1})^{-1}(-b)+b$$

が恒等式であることが示せればよい．そこで，さらに一般的な恒等式を導こう．（以下述べることは Bruck による．）

$$[y^{-1}-(y+z^{-1})^{-1}][y(zy)+y]=t \text{（ただし，} y\neq 0,\ y\neq -z^{-1}\text{）}$$

と置く．まず両辺に $y+z^{-1}$ を乗じて次の式を得る．

$$\begin{aligned}(y+z^{-1})t&=(y+z^{-1})[zy+1-(y+z^{-1})^{-1}(y(zy))-(y+z^{-1})^{-1}y]\\&=y(zy)+y+y+z^{-1}-y(zy)-y\\&=y+z^{-1}.\end{aligned}$$

したがって $t=1$ であり，$y^{-1}-(y+z^{-1})^{-1}$ と $y(zy)+y$ は互いに他の逆元になっている．それゆえ各元 x に対して，

$$[y^{-1}-(y+z^{-1})^{-1}][(y(zy))x+yx]=x$$

である．いま，

$$[y^{-1}-(y+z^{-1})^{-1}][y(z(yx))+yx]=w$$

と置けば，

$$\begin{aligned}(y+z^{-1})w&=(y+z^{-1})[z(yx)+x]-y[z(yx)]-yx\\&=yx+z^{-1}x=(y+z^{-1})x\end{aligned}$$

したがって $w=x$ である．したがって以上の2式を比較して，

$$(M)\qquad [y(zy)]x=y[z(yx)]$$

（Moufang 恒等式）を得る．この式は任意の $y\neq 0$, $y\neq -z^{-1}$ に対して成り立ったわけだが，$y=0$, $y=-z^{-1}$ に対しても，もちろん成り立つ．ここで，特に $z=1$ を代入すれば，左交代律

$$(LA)\qquad (yy)x=y(yx)$$

を得る．

任意の直線に関して移行平面である平面を **Moufang 平面**とよぶ．この名称は Ruth Moufang [1] が，この平面を最初に研究したことによる．

定理 20.5.3. 平面が Moufang 平面であるための必要十分条件は，その平面を座標づけるすべての三元環が次の条件 1)，2) を満たすことである．

1) 線型条件

2) 交代環である．すなわち，次の条件 2.1)〜2.7) を満たす．

2.1) 加法はアーベル群を作る

2.2) $(a+b)m=am+bm$

2.3) $a(s+t)=as+at$

2.4) 各 $a\neq 0$ は，$a^{-1}a=aa^{-1}=1$ を満たす逆元 a^{-1} を持つ．

2.5) $a^{-1}(ab)=b$

2.6) $(ba)a^{-1}=b$

2.7) $a(ab)=(aa)b$，$(ba)a=b(aa)$（交代律）

証：（必要条件）定理 20.5.2 から (2.1)〜(2.5) が成り立つことは明らか．右交代律 $(ba)a=b(aa)$ は (2.5) から，左交代律は (2.6) から直ちに導かれるから，(2.6) を証明すれば必要条件の証明は完成する．

軸が $y=0$，中心が $(0,0)$ でかつ $Y=(\infty)$ を $(0,-1)$ へ移すような相応を考えれば，

$$(\infty)\longrightarrow(0,-1)$$
$$(1,0)\longrightarrow(1,0)$$

であるから，

$$x=1\longrightarrow y=x-1$$

が成り立つ．また，

$$(\infty)\longrightarrow(0,-1)$$
$$(a,0)\longrightarrow(a,0)$$

であるから，

$$x=a\longrightarrow y=xa^{-1}-1$$

が成り立つ．また，

$$x=1\longrightarrow y=x-1$$
$$y=x(1-ab)\longrightarrow y=x(1-ab)$$

であるから，

$$(1, 1-ab) \longrightarrow [(ab)^{-1}, (ab)^{-1}-1]$$

が成り立つ．また，

$$(0) \longrightarrow (0)$$

であるから

$$x=a \longrightarrow y=(ab)^{-1}-1$$

である．また，

$$y=1-ab \longrightarrow y=(ab)^{-1}-1$$

$$x=a \longrightarrow y=xa^{-1}-1$$

$$y=x(a^{-1}-b) \longrightarrow y=x(a^{-1}-b)$$

であるから，

$$(a, 1-ab) \longrightarrow (b^{-1}, b^{-1}a^{-1}-1)$$

である．また，

$$(0) \longrightarrow (0)$$

であるから，

$$y=1-ab \longrightarrow y=b^{-1}a^{-1}-1$$

が成り立つ．

ここで $y=1-ab$ の像を比べれば $(ab)^{-1}=b^{-1}a^{-1}$ が成り立つ．したがって

$$\begin{aligned} b &= (b^{-1})^{-1} = [a(a^{-1}b^{-1})]^{-1} \\ &= (a^{-1}b^{-1})^{-1}a^{-1} \\ &= (ba)a^{-1}. \end{aligned}$$

すなわち，(2.6) は証明された．

(十分条件) 交代環が与えられていると仮定する．このとき，その交代環によって座標づけられた平面を作れば，定理 20.5.2 により，この平面は $Y=(\infty)$ を通る各直線に関して移行平面である．それゆえ定理 20.5.1 とその系から分かるように十分条件を証明するためには，$Y=(\infty)$ を動かす共線変換の存在がいえればよい．ところで，次の写像（すなわち x 座標と y 座標を取り換える写像）は求めているものである．

$$(a, b) \rightleftarrows (b, a)$$

$$(0) \rightleftarrows (\infty)$$
$$(m) \rightleftarrows (m^{-1}), \quad m \neq 0$$
$$x=c \rightleftarrows y=c$$
$$y=xm+b \rightleftarrows y=xm^{-1}-bm^{-1}, \quad m \neq 0$$

証終.

この定理で述べたことよりさらに詳しい結果が得られているが，その証明には交代環に関する詳しい研究を必要とするので，ここでは結果だけを述べる.

平面が相異なる2直線に関して移行平面であれば，その平面は Moufang 平面になる（すなわち任意の直線に関して移行平面である）. このことは，交代律 (2.6) $(ba)a^{-1}=b$ が先行する規則から代数的に導かれるということを意味する. しかしこのことの簡単な証明を著者は知らない. 一方すでに見たように，左交代律 $x(xy)=(xx)y$ は (2.5) から導かれた. Kleinfeld [2] と Skornyakov [2] は，標数が2でない場合には，左交代律から右交代律が（可逆環において）導かれることを示した. このことは標数が2の場合には一般に成り立たないが，San Soucie は (2.5) から導かれた Moufang 律 $[y(zy)]x=y[z(yx)]$ という仮定があれば，たとえ標数が2であっても，上のことが成り立つことを示した. Bruck-Kleinfeld [1] は交代環に関する詳しい研究を行ない，交代環 R は結合的であるか，あるいは体 F を中心とするその上のある種の多元環であるというすばらしい結果を得た. すなわち，その多元環 R は，F 上の Cayley-Dickson 多元環とよばれ，8個の基底となる元を持ち，R の任意の2元（ただし F の同じ2次拡大体に含まれない）が，四元数環を生成する. この研究をさらに進めることにより，Moufang 平面においては，その各座標環がすべて（交代環であるというばかりでなく）同型であるということも分かる. これらのことに関する詳しい話（San Soucie の結果を除いた）については Pickert [1] を参照.

定理 20.5.4. 平面 π において，次の条件 1) と 2) は同値である.

1) π は X-OY 可移である. すなわち π は中心 $X=(0)$ 軸 $x=0$ なるす

べてのホモロジーを含む.

2) 平面 π の 4 点 X, Y, O, I により定まる三元環において 2.1) $x\cdot m\circ b = xm+b$ でありかつ 2.2) 乗法は群を作る.

証：平面 π において（1）が成り立つと仮定する. 軸 $x=0$ 中心 $X=(0)$ で L_∞ 上の 1 点 (m) を（1）へ移すホモロジーを考えれば,

$$(0, 0) \longrightarrow (0, 0)$$

$$(m) \longrightarrow (1)$$

したがって

$$y=xm \longrightarrow y=x$$

である. 一方,

$$y=am \longrightarrow y=am$$

であるから

$$(a, am) \longrightarrow (am, am)$$

である. また,

$$(\infty) \longrightarrow (\infty)$$

であるから

$$x=a \longrightarrow x=am$$

$$y=c \longrightarrow y=c$$

したがって

$$(a, c) \longrightarrow (am, c)$$

である. また,

$$(0, b) \longrightarrow (0, b)$$

$$(m) \longrightarrow (1)$$

であるから

$$y=x\cdot m\circ b \longrightarrow y=x+b$$

である. したがって, もし (a, c) が $y=x\cdot m\circ b$ 上にあれば, (am, c) は $y=x+b$ 上にある. したがって $c=a\cdot m\circ b$ から $c=am+b$ が導かれるから, $a\cdot m\circ b=am+b$ であり, 線型条件 (2.1) は成り立つ.

一方この

$$(m) \longrightarrow (1)$$

なるホモロジーにより，

$$(a, 1) \longrightarrow (am, 1)$$

であるから特に

$$(1, 1) \longrightarrow (m, 1)$$

である．また，$(n) \to (1)$ なるホモロジーをさらにほどこすことにより

$$(1, 1) \longrightarrow (m, 1) \longrightarrow (mn, 1)$$

$$(a, 1) \longrightarrow (am, 1) \longrightarrow ((am)n, 1)$$

を得る．したがってこれ等2つのホモロジーの積は，$(nm) \to (1)$ なるホモロジーでなければならない．したがって $(am)n = a(mn)$ であり，乗法に関する結合律は成り立つ．ところで，乗法はループを作っていたから，乗法は群を作る．すなわち（2.2）は成り立つ．

逆に，条件（2）が成り立つと仮定する．与えられた $m \neq 0$ に対して，

$$(\infty) \longrightarrow (\infty)$$

$$(0) \longrightarrow (0)$$

$$(n) \longrightarrow (m^{-1}n)$$

$$(a, b) \longrightarrow (am, b)$$

$$L_\infty \longrightarrow L_\infty$$

$$x = a \longrightarrow x = am$$

$$y = xn + b \longrightarrow y = x(m^{-1}n) + b$$

で定められた写像は，平面 π のホモロジーである．したがって m を任意に動かせば，中心 $X = (0)$，軸 $x = 0$ なるホモロジーはすべて存在するから，条件（1）は成り立つ．証終．

定理 20.5.5. 平面 π において，部分的なデザルグの定理である，次の条件 1)，2) が成り立っていると仮定する．

1) 1点を通らない任意の3直線を軸として，線型定理が常に成り立つ．

2) ある軸とその上にないある中心に対して，デザルグの定理が成り立つ.

このとき，π を座標づける三元環として結合的な可逆環（division ring）がとれる．さらに，デザルグの定理は π 全体で成り立ち，π の共線変換群は，quadrilateral（一般の位置にある4角形）の集合の上に可移である．また，π の各三元環はいずれも結合的な可逆環（division ring）であり，互いにすべて同型である.

証：仮定から，定理 20.5.3 および定理 20.5.4 を適用することができる．したがって，一般の位置にある4点 X, Y, O, I を適当に選ぶことにより，π の三元環が定まるが，このとき $x \cdot m \circ b = xm + b$ が成り立ち，この座標環は結合的な division ring である．もし一般の位置にある4点 X_1, Y_1, O_1, I_1 を，一般の位置にある4点 X_2, Y_2, O_2, I_2 へこの順序に従って，写すような π の共線変換が存在すれば，明らかに，それらから定まる2つの三元環は互いに同型である．まず，平面 π のある一般の位置にある4点 X_1, Y_1, O_1, I_1 に対する座標環が結合的な可逆環（division ring）D であれば，π の共線変換群が quadrilateral（一般の位置にある4角形）の集合の上に可移であることを示す．いま，定理 20.5.3 により，π はすべての直線に関して移行平面である．そこで三角形 ABC が与えられたとき，AB を軸とし C を AB 上にない任意に選んだ点 C' へ移すような相応が存在する．したがって，任意の quadrilateral $X_2Y_2O_2I_2$ から出発して X_2 を X_1 へ，Y_2 を Y_1 へ，O_2 を O_1 へ移す共線変換が存在する．点 I_2 は三角形 $X_2Y_2O_2$ のいずれの辺の上にもないから，I_2 は有限の点である．すなわち $I_2=(a, b)$, $a \neq 0$, $b \neq 0$ と表わされる．このとき，次の共線変換は X, Y, O を固定し I_2 を I_1 へ移す.

$$(x, y) \longrightarrow (xa^{-1}, yb^{-1})$$

$$(m) \longrightarrow (amb^{-1})$$

$$(\infty) \longrightarrow (\infty)$$

$$y = xm + s \longrightarrow y = x(amb^{-1}) + sb^{-1}$$

$$x = c \longrightarrow x = ca^{-1}$$

$$L_\infty \longrightarrow L_\infty$$

以上のことから分かるように，各座標環はいずれも同型な可逆環Dでありπの共線変換群は quadrilateral の集合の上に可移である.

次に，デザルグの定理がπ全体で成り立つことを示す．πは可能なすべての相応を含むから，もし中心が軸の上にあれば問題はない．そこで，中心が軸の上にないと仮定する．さて，中心としてO，軸としてL_∞をとる．このとき中心O，軸L_∞のホモロジーが存在することを示そう．いま$a\neq 0$を固定して，次の写像を考える.

$$(\infty) \longrightarrow (\infty)$$
$$(m) \longrightarrow (m)$$
$$(c, d) \longrightarrow (ac, ad)$$
$$L_\infty \longrightarrow L_\infty$$
$$x=c \longrightarrow x=ac$$
$$y=xm+b \longrightarrow y=xm+ab.$$

この写像は求めていたホモロジーである．そこでaを0以外のすべての元にわたって動かすことにより中心O，軸L_∞の可能なすべてのホモロジーを得る．証終.

20.6. Wedderburn の定理と Artin-Zorn の定理

まず，以下で必要となる有限体の幾つかの性質について述べる．証明は Van der Waerden [1] vol. 1 Chap. V. §37 を参照.

1) 有限体の元の個数は素数の巾であり，各素数巾p^rに対してp^r個の元からなる有限体$GF(p^r)$が同型を除き，一意的に存在する.

2) $GF(p^r)$の各元xは$x^{p^r}=x$なる関係を満たす．$GF(p^r)$の零元0を除いたp^r-1個の元からなる乗法群$GF^*(p^r)$は巡回群である．この巡回群の生成元を原始根とよぶ.

3) $GF(p^r)$は，p個の元からなる素体F_pを係数とする多項式環の，F_p上の次数がrであるような1つの既約多項式$f(x)$による剰余類と見なすこと

ができる．いい換えれば，$GF(p^r)$ は有理整数係数多項式環のイデアル $[p, f(x)]$ による剰余類と見なすことができる．

4）体 $GF(p^r)$ の自己同形は位数 r の巡回群を作り，自己同型 $z \to \alpha(z) = z^p$ はその生成元となる．

定理 20.6.1.（Wedderburn の定理） 有限斜体 R は常に可換であり，有限体 $GF(p^r)$ である．

証：以下の証明は Witt [1] による．R の単位元で主成される部分環は R の特性部分体（すなわちすべての自己同型により不変な部分体）であり，これはある素数 p に対する有限体 F_p でなければならない．R の F_p 上の基底を $x_1 = 1, x_2, \cdots, x_r$ とすれば，Rはちょうど p^r 個の元を含む．R の中心 Z は $zx = xz$ が任意の $x \in R$ に対して成り立つようなRの元 z 達の集合で，Zは可換な有限体である．Z が $q = p^s$ 個の元からできていると仮定する．以下の目標は $Z = R$ を示すことである．いずれにせよ，RはZ上のベクトル空間だから，RのZ上の基底が t 個だと仮定してよい．したがって，$q^t = p^{st} = p^r$ である．Rにおける元 x と可換な元の作る集合 N_x はRの部分環となり，しかもZを含む．したがって N_x は q^d 個の元から成っている体である．また，R は N_x 上のベクトル空間だから $d|t$ が成り立つ．したがって，Rから0を除いた $p^r - 1 = q^t - 1$ 個の元からなる乗法群 R^* において，$x \notin Z$ なる元 x の正規化群 N_x の位数は $q^d - 1$ である（このとき $d|t, d<t$）．したがって R^* の元の個数は，

$$q^t - 1 = q - 1 + \sum \frac{(q^t-1)}{(q^d-1)} \tag{20.6.1}$$

個である．ここで $q-1$ は中心Zに含まれる元の数を表わし，残りは $(q^t-1)/(q^d-1)$ 個づつのクラスに分かれる（$d|t, d<t$）．

§16.8 で示したように，多項式 $f(x) = x^t - 1$ は，整数係数多項式 $k(x) = \prod(x - w^j)$（w は1の原始 t 乗根，$j = 1, \cdots, t$，$(j, t) = 1$）を因数に持つ．したがって，$d|t, d<t$ かつ $k(x)$ は $(x^d - 1)$ と共通の根を持たないから $x^t - 1 = k(x) \cdot (x^d - 1) \cdot r(x)$（$r(x)$ は整数係数多項式）と表わされる．したがって，

$(x^t-1)/(x^d-1)=k(x)\cdot r(x)$ である．$x=q$ を代入すれば $k(q)=\prod_{(j,t)=1}(q-w^j)$ であり $w^j\neq 1$ は1の（複素）原始 t 乗根であるから $|q-w^j|>q-1$ である．したがって，$k(q)$ の値は整数で，その絶対値は $q-1$ 以上である．したがって，もし $t>1$ であれば $k(q)$ は（20.6.1）における $q-1$ 以外の項をすべて割るから $k(q)$ も $q-1$ を割る．しかし $|k(q)|>q-1$ であるから矛盾である．したがって $t=1$，したがって $Z=R$ でなければならない．ゆえに，Rは可換で，Rは有限体である．証終．

代数系 R に加法および乗法とよばれる2つの二項演算が定義され次の条件1)，2)，3）を満たしているとき，Rを**交代環**（alternative ring）とよぶ．すなわち，

1）加法はアーベル群である．

2）左，右分配律が成り立つ．

3）乗法は次の弱い意味での結合律を満たす．すなわち，

(20.6.1) $$(xx)y=x(xy),\quad y(xx)=(yx)x.$$

さらに，Rの0と異なる元全体が乗法に関してループを作るとき，Rを交代可逆環（alternative division ring）とよぶ．前節では Moufang 平面の座標環として交代可逆環が取れることを示した．またそこでは，（20.6.1）のかわりに次の乗法律

(20.6.2) $$aa^{-1}=a^{-1}a=1$$
$$a^{-1}(ab)=b=(ba)a^{-1}$$

を用いたが，（20.6.1）は（20.6.2）から導かれるということもすでに示した．以下の目標は有限交代可逆環は有限体であるという Artin-Zorn の定理を示すことである．まずここでは交代環に関する幾つかの理論を述べる．これ等のうちのあるものは Artin-Zorn の定理を証明するためには直接必要ではないが，それ自身としても興味深いと思われる．

次に，一般に分配律の成り立つような任意の環に対して**結合子**（x, y, z）と**交換子**（x, y）とよばれるものを，

(20.6.3) $$(x, y, z)=(xy)z-x(yz)$$

$$(x, y)=xy-yx$$

で定義する．定義から明らかなように，結合的な環においては結合子は常に0であり，可換な環においては交換子は常に0である．明らかに結合子，交換子は共に各変数に関して線型である．結合子を用いれば（20.6.1）は次の式に書き直される．

(20.6.4)
$$(x, x, y)=0,\quad (y, x, x)=0$$

結合子の各変数に対する線型性により

(20.6.5)
$$\begin{aligned}0&=(x, y+z, y+z)\\&=(x, y, y)+(x, y, z)+(x, z, y)+(x, z, z)\\&=(x, y, z)+(x, z, y)\\0&=(x+y, x+y, z)\\&=(x, x, z)+(x, y, z)+(y, x, z)+(y, y, z)\\&=(x, y, z)+(y, x, z)\end{aligned}$$

が成り立つ．したがって，

(20.6.6)
$$\begin{aligned}(x, y, z)&=-(x, z, y)=(z, x, y)=-(z, y, x)\\&=(y, z, x)=-(y, x, z)\end{aligned}$$

が成り立つ．すなわち，x, y, z に偶置換（x, y, z 上の対称群の元で交代群に属するもの）を作用させても (x, y, z) は不変であり，奇置換を作用させれば (x, y, z) は符号のみかわる．交代環という名称はこの事実に由来している．(20.6.6) により $(x, y, x)=-(x, x, y)=0$ である．したがって

(20.6.7)
$$(xy)x=x(yx)$$

が成り立つ．この規則（20.6.7）を**反射律**とよぶ．

関数 $h(x_1, \cdots, x_n)$ が**歪対称関数**であるとは，次の性質（1），（2）が成り立つことをいう．

（1） 各変数に対して線型．

（2） ある2つの変数が等しければ $h(x_1, \cdots, x_n)$ の値は0である．

$h(x_1, \cdots, x_n)$ が歪対称関数であれば，$h(x_1, \cdots, x_n)$ は交代関数である（すなわち $x_1, \cdots, x_n$ の偶置換により不変であり，奇置換により符号のみ変える）．特

に交代環において，結合子 (x, y, z) および交換子 (x, y) は歪対称関数である．

次に，交代環において成り立つ幾つかの公式を述べる．

次の恒等式 (20.6.8) は，分配律の成り立つ一般の環において常に成り立つ．

(20.6.8)
$$(wx, y, z)-(w, xy, z)+(w, x, yz) = w(x, y, z)+(w, x, y)z$$

いま，関数 $f(w, x, y, z)$ を，次のように定義する．

(20.6.9)
$$f(w, x, y, z)=(wx, y, z)-x(w, y, z)-(x, y, z)w$$

補題 20.6.1. 交代環 R において (20.6.9) で定義した関数 $f(w, x, y, z)$ は歪対称関数であり，次の2つの恒等式を満たす．

(20.6.10)
$$3f(w, x, y, z)=(w, (x, y, z))-(x, (y, z, w)) +(y, (z, w, x))-(z, (w, x, y))$$

(20.6.11)
$$f(w, x, y, z)=((w, x), y, z)+((y, z), w, x)$$

証：(20.6.6) を用いて，(20.6.8) を書き直せば，

(20.6.12)
$$(wx, y, z)-(xy, z, w)+(yz, w, x) = w(x, y, z)+(w, x, y)z$$

が得られる．ここで (20.6.12) の右辺を $F(x, y, z, w)$ と置いたとき，(20.6.12) を用いて計算すれば分かるように，

(20.6.13)
$$f(w, x, y, z)-f(x, y, z, w) +f(y, z, w, x)=F(x, y, z, w)$$

が成り立つ． 一方， $F(x, y, z, w)$ は式 (20.6.12) の右辺と定義したから，x, y, z を巡回的に置換したとき，符号を変える．したがって，(20.6.13) から

$$0=F(w, x, y, z)+F(x, y, z, w) =f(w, x, y, z)+f(z, w, x, y)$$

であり，

(20.6.14)
$$f(w, x, y, z)=-f(z, w, x, y)$$

が成り立つ．したがって，x, y, z, w を巡回的に置換したとき，f は符号を変える．また，(20.6.9) 式から分かるように，最後の2変数 y と z を入れ換え

たときにも符号を変える．したがって f はどの２変数を入れ換えても符号を変える．一方 $f(w, x, y, y)=0$ であるから，以上のことから分かるように f は歪対称関数である．特に，(20.6.10) は (20.6.13) から導かれる．また式 (20.6.8) から (20.6.8) の w と x を入れ換えた式を辺々引けば，

$$((w, x), y, z)=-(w, (x, y, z))+(x, (y, z, w))+2f(w, x, y, z)$$

が成り立つ．ここで (20.6.10) を用いて，(20.6.11) の右辺を計算してやれば左辺が得られる．証終．

補題 20.6.2. 交代環の任意の元 x, y, z に対して，

(20.6.15) $$(x^2, y, z)=x(x, y, z)+(x, y, z)x$$

(20.6.16) $$(x, xy, z)=(x, y, xz)=(x, y, z)x$$

(20.6.17) $$(x, yx, z)=(x, y, zx)=x(x, y, z)$$

が成り立つ．また Moufang 恒等式

(20.6.18) $$(xy)(zx)=x((yz)x)=(x(yz))x$$

(20.6.19) $$x(y(xz))=((xy)x)z, \quad ((zx)y)x=z(x(yx))$$

が成り立つ．

証：$f(x, x, y, z)=0$ から (20.6.15) が得られる．また，$f(x, y, z, x)=0$, $f(x, z, x, y)=0$ の２つの関係から (20.6.16) の２つの等式が得られる．また $f(y, x, x, z)=0$, $f(z, x, x, y)=0$ から (20.6.17) が得られる．また (20.6.17) を用いれば，

$$\begin{aligned}(xy)(zx)&=x(y(zx))+(x, y, zx)\\&=x(y(zx))+x(y, z, x)\\&=x((yz)x)\end{aligned}$$

であるから (20.6.18) が得られる．また (20.6.16) により，

$$\begin{aligned}((xy)x)z&=(xy)(xz)+(xy, x, z)\\&=x(y(xz))+(x, y, xz)-(x, xy, z)\\&=x(y(xz))\end{aligned}$$

したがって，(20.6.19) の第一番目の式が得られた．同様に，(20.6.17) か

ら，二番目の式が得られる．証終．

次に，可逆環においては(20.6.1)から(20.6.2)が導かれることを示す．さて，元 $a \neq 0$ が与えられたとき，可逆環であるという仮定から，$au=1$ なる元 u が存在する．このとき反射律が成り立つから $a=(au)a=a(ua)$ であり，したがって $ua=1$ である．そこで $u=a^{-1}$ と書くことができ，$a^{-1}a=aa^{-1}=1$ である．さて，0 でない任意の 2 元 a, b が与えられたとする．このとき $b=a^{-1}c$ なる c は一意的に定まる．したがって，(20.6.19) の第一番目の式を用いて，

$$a^{-1}(ab)=a^{-1}(a(a^{-1}c))=((a^{-1}a)a^{-1})c$$
$$=(1a^{-1})c=a^{-1}c=b$$

が得られる．同様に (20.6.19) の 2 番目の式を用いて，

$$(ba)a^{-1}=b$$

が導かれる．

いよいよ，目標である次の定理にとりかかろう．

定理 20.6.2. **(Artin-Zorn)**[*] 有限交代可逆環 R は有限体である．

証：まず，2 元 b, c から生成された有限交代可逆環 R_1 は結合的であることを証明する．もしこれがいえれば，Wedderburn の定理により，R_1 は有限体であり，したがって 1 つの元で生成される．したがって，いま R が元 b_1, $b_2, \cdots, b_s$ から生成されていれば，b_1, b_2 の生成するものは有限体であり，1 つの元 c_1 から生成される．したがって R は $c_1, b_3, \cdots, b_s$ で生成される．このようにして，順々に R の生成元の数を減らしてゆけば，最後に R は 1 つの元から生成され，したがって結合的であり，R が有限体であることが分かる．さて，R_1 が 2 元 b, c で生成されていると仮定する．このとき，R_1 は加法と乗法に関して閉じている R の部分代数系である．いま，R_1 は有限だから，零因子を持たない．そこで，$a_1, \cdots, a_t$ を R_1 の 0 と異なる元全体としたとき，任意の $x \in R_1$ に対して，$xa_1, \cdots, xa_t$ はすべて相異なる．したがって，$xa_1, \cdots, xa_t$ は $a_1, \cdots$, a_t を並べ変えたものである．したがって，$xa_1=x$ を満たすある元 a_1 が存在

*) Zorn [1] 参照．

する．ここで $a_1=1$ はRの単元である．また，$xa_i=1$ を満たすある元 a_i が存在する．したがって $a_i=x^{-1}$ である．したがって R_1 は可逆環である．さて，R_1 の各元は単項式 $(x_1\cdots x_r)(x_{r+1}\cdots x_n)$（ここでカッコは任意の方法でつけられている）の和として表わされる．ここで x_i は b または c のいずれかである．ところで，左右の分配律は成り立つから，乗法が結合的であるための必要十分条件は，単項式の間の乗法が結合的であることである．このことを示すために，（左からカッコづけられた）正規単項式とよばれるものを帰納的に次のように定義する．

(20.6.20)
$$[x_1x_2]=x_1x_2$$
$$[x_1\cdots x_n]=[x_1\cdots x_{n-1}]x_n.$$

次に，任意にカッコをつけた単項式は，それと同じ要素からなる正規単項式と等しいことを証明する．もしこれが示されれば，

$$([x_1\cdots x_r][y_1\cdots y_s])[z_1\cdots z_t]=[x_1\cdots x_r y_1\cdots y_s z_1\cdots z_t]$$
$$=[x_1\cdots x_r]([y_1\cdots y_s][z_1\cdots z_t])$$

であるから結合律は成り立つ．以下，任意の単項式がその正規単項式と等しいことを単項式の長さに関する帰納法を用いて証明する．(20.6.4) および (20.6.6) から分かるように，長さ3の b と c からなる単項式に関しては正しい．なぜならば，3つの要素のうちの少なくともある2つは同じでなければならないからである．したがって，

(20.6.21)
$$x_1(x_2x_3)=(x_1x_2)x_3=[x_1x_2x_3]$$

である．次に

(20.6.22)
$$[u_1\cdots u_r][v_1\cdots v_s]=[u_1\cdots u_r v_1\cdots v_s]$$

を $n=r+s$ と nを固定したときの s に関する帰納法を用いて証明する．$s=1$ に対して (20.6.22) は定義により正しい．まず，$s>1$, $v_1=v_s=b$ かつ $v_1=v_s=c$ と仮定する．このとき，(20.6.19) の二番目の式 $z[x(yx)]=[(zx)y]x$ において，$z=[u_1\cdots u_r]$, $v_1=v_s=x$, $[v_2\cdots v_{s-1}]=y$ と置く．このとき，帰納法を用いて，

(20.6.23)
$$[u_1\cdots u_r][xv_2\cdots v_{s-1}x]=\{([u_1\cdots u_r]x)[v_2\cdots v_{s-1}]\}x$$
$$=[u_1\cdots u_r u_1 v_2\cdots v_{s-1}]v_s$$

$$=[u_1\cdots u_r v_1 v_2\cdots v_{s-1}v_s]$$

が得られる．したがって，$v_1=v_s$ のとき，(20.6.22) は示された．いま，$v_1\neq v_s$ と仮定する．ここで $v_1=b$, $v_s=c$ として一般性を失わない．$u_r=b$ または c であるが，まず $u_r=b$ であると仮定する．そこで，$x=[u_1\cdots u_{r-1}]$, $u_r=b$, $v_1=b$, $[v_2 y_s]=y$ と置く．$f(x,b,b,y)=0=(xb,b,y)-b(x,b,y)-(x,b,b)y$ である．ここで，$(x,b,b)=0$ であり，また，長さに関する帰納法により，x, b, y に関して結合的である．したがって $(x,b,y)=0$ が成り立つ．したがって $(xb,b,y)=0$ であり，したがって $(xb)(by)=[(xb)b]y$ である．すなわち，

$$(20.6.24)\qquad [u_1\cdots u_{r-1}b][bv_2\cdots v_s]=([u_1\cdots u_{r-1}]bb)[v_2\cdots v_s]$$
$$=[u_1\cdots u_{r-1}bb][v_2\cdots v_s]$$
$$=[u_1\cdots u_r v_1\cdots v_s]$$

である．ここで s に関する帰納法を最後の変形のところで用いた．次に，$u_r=c$ であると仮定する．

$$x=[u_1\cdots u_{r-1}],\quad u_r=c,\quad [v_1\cdots v_{s-1}]=z,\quad v_s=c$$

と置く．いま，$f(x,c,z,c)=0=(xc,z,c)-c(x,z,c)-(c,z,c)x$ である．ここで，$(c,z,c)=0$ であり．また長さに関する帰納法を用いることにより，$(x,z,c)=0$ を得る．したがって $(xc,z,c)=0$ であるから $(xc)(zc)=[(xc)z]c$ である．すなわち，

$$(20.6.25)\qquad [u_1\cdots u_{r-1}c][v_1\cdots v_{s-1}c]=([u_1\cdots u_{r-1}c][v_1\cdots v_{s-1}])c$$
$$=[u_1\cdots u_{r-1}u_r v_1\cdots v_{s-1}]c$$
$$=[u_1\cdots u_{r-1}u_r v_1\cdots v_{s-1}v_s]$$

である．以上の式 (20.6.23, 24, 25) から，(20.6.22) はいずれの場合にも成り立つことが示された．したがって R_1 は結合的である．証終．

20.7. 2重可移群と擬体 (near-field)

射影平面と密接に結びついているような有限群達の1つのクラスを考える．すなわち，2重可移群で2文字以上を固定する元は単位元に限るという性質を持った群について考察する．この際，さらに仮定 3) または 3′) を加える．こ

の仮定はあるいは不必要なのかも知れないが，以下の我々の証明においては省くことができない．

定理 20.7.1. G は n 個の文字 $c_0, c_1, \cdots, c_{n-1}$ の上の置換群で次の条件 1)，2)，3）または 1)，2)，3'）を満たすと仮定する．

1） G は2重可移．

2） 2文字以上を固定する G の元は単位元に限る．

3） G の元で c_i を c_j に移し，各文字をすべて動かすものはたかだか1つである．

3'） n は有限．

このとき，すべての文字 c_i を動かすような G の元の全体は群を作る．この群はアーベル群で G の正規部分群である．さらに，群 G はある擬体 K における $x \to mx+b$ なる線型変換全体の作る群と同型になる．逆に，擬体 K において $x \to mx+b$, $m \neq 0$ なる線型変換全体の作る群は K の元の集合の上の置換とみたとき，条件 1), 2）を満たす．もし $m \neq 0, 1$ に対して，$xm+b=x$ が常にただ一つの解を持つならば，条件 3）も満たされ，擬体 K で座標づけられた射影平面の有限直線達として $x=c$, $y=xm+b$ をとることができる．このとき，K の元の上での置換と見た G の元 $\begin{pmatrix} c_0, & c_1, & \cdots, & c_{n-1} \\ d_0, & d_1, & \cdots, & d_{n-1} \end{pmatrix}$ は，(c_i, d_i), $i=0, \cdots, n-1$ という点の集合からなる π の直線と対応づけられる．

証：まずこの定理の純群論的な部分，すなわち，すべての文字を動かすような G の元全体と単位元とを合わせたものが可換な正規部分群を作ることを示す．

補題 20.7.1. 相異なる2つの文字 i, j を交換するような G の位数2の元は存在し，ただ一つである．

証：G は2重可移であるから，i, j を交換するような元 g は存在する．このとき，g^2 は2文字 i, j を固定するから，単位元であり，したがって g の位数は

2である．さらに元hもこの性質を満たしているとすれば，gh^{-1}は2文字i, jを固定するから単位元，したがって $g=h$ である．証終．

補題 20.7.2. 群Gの位数2の元はすべて共役である．

証：$n=2$ ならば，位数2の元はただ一つしかないから自明である．したがって $n\geqq 3$ と仮定してよい．g, h をいずれも位数2の元とすれば，g およびhにより動かされるようなある文字iが存在する．（すなわち $g=(i, j), \cdots, h=(i, k)\cdots$.）このとき，$G$の元 $x=\begin{pmatrix} i, & j, & \cdots \\ i, & k, & \cdots \end{pmatrix}$ が存在して，$x^{-1}gx=(i, k)\cdots$ となる．したがって補題20.7.1により $x^{-1}gx=h$ である．証終．

この補題から分かるように，次の2つの場合のどちらか一方のみが必ず起こる．

Case 1. 位数2の任意の元はすべての文字を動かす．

Case 2. 位数2の任意の元はある1文字を固定する．

補題 20.7.3. Case 2. において，与えられた1文字を固定する位数2の元はただ一つ存在する．

証：前にみたように元 g, h が共に位数2で，$g=(i, j)\cdots$, $h=(i, k)\cdots$ ならば，元 $x=\begin{pmatrix} i, & j, & \cdots \\ i, & k, & \cdots \end{pmatrix}$ が存在して，$x^{-1}gx=h$ が成り立つ．もしgとhが共に同一の文字sを固定したとすれば，xもsを固定する．したがってxはiとsを共に固定するから $x=1$，したがって $g=h$ である．一方，もしgが文字sを固定すれば，他の任意の文字tに対して，tを固定する位数2の元は，sをtに移すような元でgを変換することにより得られる．証終．

この補題から分かるように，$g=(i, j)(s)\cdots$ であれば，gは，文字sを固定するようなGの元全体からなる部分群 H_s の中心に属する．

補題 20.7.4. 位数2の相異なる2つの元の積はすべての文字を動かす．

証：$g^2=1$, $h^2=1$, $g\neq h$ でかつ，gh が文字iを固定したと仮定する．補題

20.7.3により，g, h の両方が i を固定することはない．一方，gh は i を固定するから g, h のどちらも i を固定することはできない．したがって，$g=(i, j), \cdots$, $h=(j, i)\cdots$ であるが，$gh^{-1}=(i)(j)\cdots=1$. したがって $g=h$ となり仮定に反する．証終.

補題 20.7.5. 文字 i を文字 $j(\neq i)$ に移し，すべての文字を動かすような G の元はただ一つ存在する.

証：Case 1. においては元 $g=(i, j)\cdots$ は上の条件を満たし，Case 2. においては $g=(i)\cdots$, $g^2=1$, $h=(i, j)\cdots$ とし，元 gh をとれば，gh は i を j に移し，かつ補題20.7.4によりすべての文字を動かす．したがって上の条件を満たす G の元が少なくとも1つ存在する．一方，仮定 3）はこの条件を満たす元がたかだか1つであることを主張している．また，仮定 3′）もこの条件を満たす元がたかだか1つであることを主張する．これを以下で示す．群 G は n 文字の上に2重可移だから，文字 C_0 を固定する G の部分群 H_0 は残りの $n-1$ 文字の上で可移で，$|G:H_0|=n$ である．さらに，G の2文字を固定する元は単位元に限るから，H_0 の位数は $n-1$, したがって G の位数は $n(n-1)$ である．したがって，文字 i を j へ移す G の元全体は，文字 i を固定する部分群 H_i による，1つの左剰余類を作り，したがって $n-1$ 個の元からなる．一方，G の2重可移性により与えられた三文字 i, j, k に対して G の元 $g=\begin{pmatrix} i, & k, & \cdots \\ j, & k, & \cdots \end{pmatrix}$ が一意的に定まる．このとき，与えられた文字 i, j に対して k の選び方はちょうど $n-2$ 通りある．したがって文字 i を j に移し，かつすべての文字を動かす元はちょうど $(n-1)-(n-2)=1$ 個である．証終.

補題 20.7.6. Case 1. において，すべての文字を動かす元はすべて位数2であり，それらの元全部と単位元を合わせたものは可換な正規部分群を作る.

証：明らかに $g=(i, j)$ は i を j に移し，すべての文字を動かす唯一の元である．このとき，g の位救は2である．もし，$g^2=1$, $h^2=1$ であれば，i）$g=h$ のとき $gh=1$ となり ii）$g\neq h$ ならば gh はすべての文字を動かすから位数

2すなわち $(gh)^2=1$ である．したがっていずれの場合も $hg=gh$ である．したがって位数2の元全体（すなわち，すべての文字を動かす元全体）と単位元の作る群 A はアーベル群である．補題20.7.2により A は G の正規部分群である．証終．

補題 20.7.7. Case 2. において，すべての文字を動かすような元 g は，2つの位数2の元 a, b を適当に選ぶことにより $g=ab$ と表わすことができる．ここで，a, b のどちらか一方は任意に選ぶことができる．

証：$a^2=1$ かつ a は文字 i を固定し，また元 g が文字 i を j に移すと仮定する．次に $b=(i, j)\cdots$ なる元をとれば，$b^2=1$ であり，かつ補題20.7.4により元 ab は文字 i を j に移しすべての文字を動かすから，$g=ab$ である．同様に位数2の元 b が k を固定し，g が i を k に移すと仮定すれば，$a=(i, k)\cdots$ をとれば $g=ab$ である．証終．

補題 20.7.8. Case 2. において，位数2の3つの元 a, b, c の積 abc は位数2であり，$abc=cba$ が成り立つ．

証：$a=b$ のとき，この主張は明らかである．$b\neq a$ であれば補題20.7.7により，元 $ab=g$ は，$ab=g=dc(d^2=1)$ と表わされる．したがって，$abc=dc^2=d$ である．また $d=d^{-1}$ であるから，$abc=c^{-1}b^{-1}a^{-1}=cba$ である．証終．

補題 20.7.9. Case 2. において，すべての文字を動かす元全体と単位元をあわせたものは，G の可換な正規部分群を作る．

証：元 g, h はすべての文字を動かすとする．補題20.7.7により，位数2の元 a, b, c, d を適当に選んで $g=ab$, $h=cd$ と表わすことができる．そこで $a=eb$, $e^2=1$, と表わせば，$gh^{-1}=ae$ である．したがって，もし $e=a$ であれば，$gh^{-1}=1$ であり，もし $a\neq e$ であれば gh^{-1} はすべての文字を動かす．したがって，すべての文字を動かす元の全体と単位元からなる集合 A は G の部分群である．そこで，補題20.7.8を用いれば，$gh=(abc)d=(cba)d=c(bad)$

$=c(dab)=hg$ である．したがって，Aはアーベル群である．また，ある元がすべての文字を動かせばそれにGの内部自己同型をほどこしたものも，やはりすべての文字を動かす．したがってAは正規部分群である．証終．

以上で定理の最初の部分の証明は終った．次の目標は群Gから擬体Kを構成することである． S を文字 $c_0, c_1, \cdots, c_{n-1}$ からなる集合とする． 特に $c_0=0$, $c_1=1$ と表わすことにする．次に，Sに対して加法

(20. 7. 1) $$y=x+b$$

を，部分群Aが

(20. 7. 2) $$A_b=\begin{pmatrix}0, & \cdots, & x, & \cdots\\ b, & \cdots, & y, & \cdots\end{pmatrix}$$

なる元を持つこととして定義する．また乗法

(20. 7. 2) $$y=xm$$

を，（0を固定するGの部分群）H_0 が

(20. 7. 4) $$M_m=\begin{pmatrix}0, & 1, & \cdots, & x, & \cdots\\ 0, & m, & \cdots, & y, & \cdots\end{pmatrix}$$

なる元を持つこととして定義する．このとき部分群Aにおいて文字0をbに移す元はただ一つ存在するからSの加法の定義は意味を持つ．また部分群 H_0 において，$m\neq 0$ ならば文字1をmに移す元はただ一つ存在するから，Sにおける乗法の定義は $m\neq 0$ に対して意味を持つ．部分群Aが次の二つの元

(20. 7. 5) $$A_a=\begin{pmatrix}0, & \cdots, & x, & \cdots\\ a, & \cdots, & y, & \cdots\end{pmatrix}$$
$$A_b=\begin{pmatrix}0, & \cdots, & a\cdots y\\ b, & \cdots, & c\cdots z\end{pmatrix}$$

を持つとき，

(20. 7. 6) $$A_aA_b=A_c=\begin{pmatrix}0, & \cdots, & x, & \cdots\\ c, & \cdots, & z, & \cdots\end{pmatrix}$$

である．したがって，加法の定義から，

(20. 7. 7) $$c=a+b,\quad y=x+a,\quad z=y+b,\quad z=x+c$$

を得る．したがって，Sの加法に関する結合律

(20. 7. 8) $$(x+a)+b=x+(a+b)$$

が成り立つ．また，Gの単位元は $A_0=\begin{pmatrix}0, \cdots, 1, \cdots, x, \cdots \\ 0, \cdots, 1, \cdots, x, \cdots\end{pmatrix}$ であるから，

(20.7.9)
$$x+0=0+x=x$$

である．また，$A_u=\begin{pmatrix}0, \cdots, a, \cdots \\ u, \cdots, 0, \cdots\end{pmatrix}$ であれば，$a+u=0$，したがって $u=-a$ である．さらにAはアーベル群であるから，$A_aA_b=A_bA_a=A_c$，したがって

(20.7.10)
$$c=a+b=b+a$$

が成り立ち，Sの加法は可換である．以上のことから分かるように，Sの加法はアーベル群を作り，対応 $a \rightleftarrows A$ により，群Aと同型である．次に部分群 H_0 を考えることにより，同様にしてSの0と異なる元全体は乗法に関して群を作ることが示される．記号0に対する乗法に関して，$0\cdot m=0$，($m\neq0$) は定義から得られるが，さらに，任意の元mに対して $m\cdot 0=0$ と定めることにする．特に $0\cdot 0=0$ である．いまgをGの任意の元とする．もし，$(0)g=b$ であれば，$g_1=gA_b^{-1}$ と書くとき，g_1 は文字0を固定するから H_0 の元であり，$g_1=M_m$ と表わされる．したがって，

(20.7.11)
$$g=M_mA_b.$$

と表わすことができる．したがって，もし $(x)g=y$ であれば，

(20.7.12)
$$(x)g=y=xm+b,\quad m\neq0$$

と表わされる．このとき（20.7.11）における g の表わし方は一意的である．なぜならば群Aと H_0 に共通なGの元は単位元だけであるからである．したがってGの元は（20.7.12）からわかるように，Sにおける線形変換

(20.7.13)
$$x \longrightarrow xm+b,\quad m\neq0$$

として表わすことができる．次にSにおいて分配律が成り立つことを示す．まず関係式

(20.7.14)
$$M_mM_t=M_{mt}$$
$$M_m^{-1}A_1M_m=A_m$$

が成り立つことを示す．最初の式は明らかである．後の式もGの元 $M_m^{-1}A_1M_m$ は，すべての文字を動かし，文字0をmに移すことから明らかである．したがって，

(20.7.15) $$M_t{}^{-1}A_mM_t=A_{mt}$$

が成り立つ．このことをSにおける演算の言葉で言い直せば，

(20.7.16) $$(xt^{-1}+m)t=x+mt$$

である．したがって $x=yt$ と置けば，分配律

(20.7.17) $$(y+m)t=yt+mt$$

が成り立つ．以上をまとめれば，Sは加法に関してアーベル群を作り，Sの0を除いた元全体は乗法に関して群を作る．またSにおいて右分配律（20.7.17）が成り立つ．したがってSは擬体である．さらに．群Gの元はSの線形変換

(20.7.18) $$x\longrightarrow xm+b,\ \ m\neq 0$$

で表わされる．特にSが擬体であることから，$\alpha: x\to xm_1+b_1$, $\beta: x\to xm_2+b_2$ とすれば

(20.7.19) $$\alpha\beta: x\longrightarrow x(m_1m_2)+b_1m_2+b_2$$

である．以上で定理の2番目の主張の証明は終った．

逆に擬体Sが与えられていると仮定する．このときSの線形変換（20.7.18）の全体は写像の合成（20.7.19）により群を作る．r, sをSの相異なる2元とするとき

(20.7.20) $$g: x\longrightarrow x(r-s)+s$$

はGの元で，$(0)g=s$, $(1)g=r$ である．したがってGは2重可移である．2文字を固定するGの元は文字0と1とを固定する元と共役になる．一方，Gの元 $x\to xm+b$ が文字0, 1を固定すれば，$b=0$, $m=1$ であり，この元は単位元である．すなわち2文字を固定するGの元は単位元以外にないことが分かった．またGの元 $x\to x+(c-b)$, $(c\neq b)$ はすべての文字を動かし，与えられた文字bをcに移す．もし，$xm+b=x$, $m\neq 0,1$ であれば，この式は常に解を持つ．したがって，すべての文字を動かす元は加法により定義される元 $x\to x+t$ に限る．このうち与えられたbをcに移すものは $x\to x+(c-b)$ ただ1つである．したがって定理の条件(3)は満たされる．このとき $(xm+b)r=xr$ または，$xs+t=xr$ は常に（したがって唯一の）解を持つ．したがって，Sを Veblen-Wedderburn 系として考えるときに，Sは，有限直線が $x=c$ と

$y=xm+b$ 達からなるようなある平面の座標系である．これで定理の証明はすべて終った．

先に注意したように，条件（3）はGが有限置換群であれば，自動的に満たされる．したがって，2点を固定する元が単位元のみであるような有限2重可移群の決定は有限擬体の決定と同値である．有限擬体は Zassenhaus [2] により完全に分類された．以下，この有限擬体の決定の概略を述べる．

Kを有限擬体とする．もしKの乗法が可換であれば，Kは分配律を満たし，Kは有限体 $GF(p^r)$ である．したがって，以下この場合は考えず，Kの乗法は非可換であると仮定する．このとき，Kは分配律を満たすことはできない．なぜならば，もし分配律を満たせば Wedderburn の定理により，Kは有限体 $GF(p^r)$ となるからである．さて，いままでの記号を用いて，Kをn個の元からなる有限擬体，GをKから得られた，2点を固定する元が単位元のみからなるような次数nの2重可移群とする．すなわち，Gは線形変換

(20.7.21) $$g : x \longrightarrow xm+b, \quad m\neq 0$$

の作る群となっている．そこで，Aを単位元とすべての文字を動かす元からなるGの部分群としたときAは可換な正規部分群である．また $H_0=M$ を文字0を固定するGの部分群と置く．このとき，AはKの加法群と同型であり，Mは K^*（K の0と異なる元全体）の乗法群と同型である．

補題 20.7.K1. Aは基本アーベル群であり，次数nは素数巾 $n=p^r$ である．さらに，Aの1と異なる元はすべてMにおいて共役である．

証：Aはアーベル群であり，さらに (20.7.14) により，$A_m=M_m^{-1}A_1M_m$ が成り立つ．したがってAの1と異なる元はすべてMで共役である．ところでAは位数がある素数pであるような元を持たなければならない．また，Aの1と異なる元はすべて共役であるから，Aの各元の位数はすべてpであり，Aは基本アーベル群である．Aは正則な位数nの置換群であるから $n=p^r$ である．証終．

補題 20.7.K2. Mの各元はAの自己同型を引き起こす．また，これ等の

（恒等写像でない）自己同型は K の 0 以外の元をすべて動かし，0 を固定する．

証：M の各元 m は $a \to am$ という K の元の置換を引き起こす．したがって，M の 1 と異なる元は加法群 A の自己同型を引き起こし，0 のみを固定する．証終．

補題 20. 7. K3. q, s が素数ならば，M の位数 q^2 または qs の部分群はすべて巡回群である．

証：$(x_1, \cdots, x_k)(x_i \in K)$ を元 M_m に対する，ある巡回置換（巡環）とする．すなわち，$x_1 m = x_2$，$x_2 m = x_3$，…，$x_k m = x_1$ である．したがって $(x_1 + \cdots + x_k)m = x_1 + \cdots + x_k$ であり，もし $m \neq 1$ であれば，$x_1 + \cdots + x_k = 0$ である．いま，M が位数 q^2 の巡回群でない部分群 W を持つと仮定する．したがって W は基本アーベル群である．さて，W が 2 元 x, y で生成されているとする．W のある一つの可移域（したがって q^2 個の文字からなる）を考えれば，x, y は次のように巡回置換の積として表わされる．

$$x = (a_1, a_2, \cdots, a_q)(a_{q+1}, \cdots, a_{2q}) \cdots (a_{q^2-q+1}, \cdots, a_{q^2}),$$

$$y = (a_1, a_{q+1}, a_{2q+1}, \cdots, a_{q^2-q+1}) \cdots (a_i, a_{q+i}, \cdots, a_{q^2-q+i}) \cdots$$

ここで，元 xy^j の a_1 を含む巡回置換は $(a_1, a_{2+jq}, a_{3+2jq}, \cdots, a_{q+j(q-1)q})$ と表わされる．したがって最初に注意したように，

$$a_1 + a_{2+jq} + \cdots + a_{q+j(q-1)q} = 0 \tag{20.7.22}$$

$$a_1 + a_{q+1} + a_{2q+1} + \cdots + a_{q^2-q+1} = 0 \tag{20.7.23}$$

が成り立つ．

そこで，(20. 7. 22) を $j = 0, 1, \cdots, q-1$ にわたってうごかし，その和をとり，さらにそれに (20. 7. 23) を加えれば

$$qa_1 + (a_1 + a_2 + \cdots + a_{q^2}) = 0 \tag{20.7.24}$$

が出る．また x の巡回置換すべてにわたっての和をとれば，

$$a_1 + a_2 + \cdots + a_{q^2} = 0 \tag{20.7.25}$$

である．したがって

$$(20.7.26) \qquad qa_1=0$$

が成り立つ．一方 M の位数は $n-1=p^r-1$ であるから，q は p と互いに素である．しかしこれは，(20.7.26) と矛盾する．したがって M は位数 q^2 の非巡回群を含むことはない．

同様に，もし M が位数 $qs(q<s)$ の非巡回群 W を含めば，W は

$$(20.7.27) \qquad x^s=1,\ \ y^q=1,\ \ q\,|\,s-1,\ \ y^{-1}xy=x^t \qquad t^q\equiv 1 \pmod{s}$$

を満たす2元 x, y から生成される．一方，M は $n-1$ 文字上に正則であるから，W は qs 個の文字からなる可移域を持つ．また，W の部分群で，位数 s のものはただ一つであり，位数 q のものは s 個存在する．これら $s+1$ 個の各群に対して，文字 a_1 を含む巡回置換を取り出して，次のようにならべる．

$$(a_1, a_2, \cdots, a_s)$$
$$(a_1, b_{11}, \cdots, b_{1,q-1})$$
$$(a_1, b_{21}, \cdots, b_{2,q-1})$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(a_1, b_{s1}, \cdots, b_{s,q-1})$$

このとき，a_1 を除いた qs 個の文字は，これ等の巡回置換の中に，ちょうど一回現われる．また a_1 は $s+1$ 回現われる．しかし，これ等 qs 個の元をすべて加え合わせたものは0である．したがって $sa_1=0$ であり，$s\,|\,p^r-1$ であるから $a_1=0$ である．これは矛盾である．したがって M は位数 qs の非巡回群を含むことはない．

補題 20.7.K4. M の位数が奇数の Sylow 部分群は巡回群である．また，M の 2-Sylow 部分群は巡回群か一般4元数群のいずれかである．

証：定理 12.5.2 で示したように，p-群 P が位数 p^2 の非巡回部分群を含まなければ，p が奇数ならば P は巡回群であり，$p=2$ ならば P は巡回群または一般4元数群である．証終．

いま，M が，M/C が巡回群となるような巡回正規部群 C を持つと仮定する．補題 20.7.K4 と定理 9.4.3 により，もし M が，一般 4 元数群であるような 2-Sylow 部分群を持たないならば，M はこの性質を満たし，また，M が一般 4 元数群と位数が奇数の部分群の直積である場合にも M はこの性質を満たす．次の定理 20.7.2 は M がこの性質を持つような有限擬体 K をすべて決める．その他に，次に示す 7 つの例外的な擬体があり，有限擬体はそれでつきることを Zassenhaus が示した．この証明に関しては Zassenhaus の原論文を参照のこと．

定理 20.7.2. $q=p^h$ を素数 p の巾，v をその約数となる素数がすべて $q-1$ を割るような整数とする．また，$q\equiv 3 \pmod 4$ ならば，$v\equiv 0 \pmod 4$ であると仮定する．ここで，$hv=r$ と置いたとき，$n=p^r$ 個の元からなる擬体 K を有限体 $GF(p^r)$ から作ることができる．

1）　K の元として $GF(p^r)$ の元をとる．

2）　K の加法として $GF(p^r)$ の加法をとる．

3）　K における積 $w\circ u$ を次のように定義する．

$GF(p^r)$ の原始根を 1 つ固定し，それを z と置く．このときもし $u=z^{kv+j}$ であれば，$q^i\equiv 1+j(q-1)[\mathrm{mod}\ v(q-1)]$ において，整数 i は v を法として一意的に定まる．そこで $w\circ u=u\cdot w^{q^i}$ と定義する．（右辺における積は $GF(p^r)$ における積を表わす．）

4）　K の中心は $GF(q)$ である．

さらに，M が M/C が巡回群になるような巡回正規部分群 C を持つような擬体 K は，すべてこのようにして構成される．

定理 20.7.2 で構成された擬体の外に，次のような例外的な 7 つの擬体が存在する．Zassenhaus は有限擬体はこれ等でつきることを示した．これら例外的な擬体の位数はすべて p^2 であり，乗法群 M の生成元を，加法群の 2 つの生成元の変換行列として与えることによって決まる．次にそれを Zassenhaus と同じ順番にあげておく．

I. $n=5^2$. $A=\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$, $B=\begin{pmatrix}1, & -2\\ -1, & -2\end{pmatrix}$

$$M\cong M(2,3)$$

II. $n=11^2$, $A=\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$, $B=\begin{pmatrix}1, & 5\\ -5, & -2\end{pmatrix}$, $C=\begin{pmatrix}4, & 0\\ 0, & 4\end{pmatrix}$

$$M\cong M(2\times 3)\times(C)$$

III. $n=7^2$, $A=\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$, $B=\begin{pmatrix}1, & 3\\ -1, & -2\end{pmatrix}$

$$M\cong G_3$$

IV. $n=23^2$, $A=\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$, $B=\begin{pmatrix}1, & -6\\ 12, & -2\end{pmatrix}$, $C=\begin{pmatrix}2, & 0\\ 0, & 2\end{pmatrix}$

$$M\cong G_3\times(C)$$

V. $n=11^2$, $A=\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$, $B=\begin{pmatrix}2, & 4\\ 1, & -3\end{pmatrix}$

$$M\cong M(2,5)$$

VI. $n=29^2$, $A=\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$, $B=\begin{pmatrix}1, & -7\\ -12, & -2\end{pmatrix}$, $C=\begin{pmatrix}16, & 0\\ 0, & 16\end{pmatrix}$

$$M\cong M(2,5)\times(C)$$

VII. $n=59^2$, $A=\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$, $B=\begin{pmatrix}9, & 15\\ -10, & -10\end{pmatrix}$, $C=\begin{pmatrix}4, & 0\\ 0, & 4\end{pmatrix}$

$$M\cong M(2,5)\times(C)$$

ここで，I の $M(2,3)$ は位数24，V の $M(2,5)$ は位数120，III の G_3 は位数48である．$M(2,5)$ の中心 Z は位数 2 であり商群 $M(2,5)/Z$ は位数60の単純群である．

20. 8. 有限平面，Bruck-Ryser の定理

位数 n の有限平面において，次のような性質 1)〜6) が成り立つことはすでに §20. 1 で示した．

1) n^2+n+1 個の直線がある．

2) n^2+n+1 個の点がある．

3）　各直線は $n+1$ 個の点を含む.

4）　各点は $n+1$ 個の直線上にある.

5）　相異なる2点を通る直線はただ一つ存在する.

6）　相異なる2直線はただ一点で交わる.

ところで, ある系が有限平面であるかどうかを示すときに, その“点”と“直線”からなる集合が上の性質のうち幾つかを満たせば実際, 位数 n の有限平面であり, 残りの性質も自動的に満たされることを知っていると便利である. 次にそれを示す.

定理 20.8.1. 点と直線の系が（1),（3),（5）または双対的に（2),（4),（6）を満たすならば, その系は位数 n の有限平面であり, さらに残りの性質も満たす.

証：系が（1),（3),（5）を満たすと仮定する. 与えられた1点 P_i を含む直線が m_i 個あるとする. この m_i 個の各直線はおのおの n 個の P_i と異なる点を含む. したがって全体で, $1+nm_i$ 個の点が存在する. そこで各点 P_i に対して, $m_i=m$ (一定) が成り立つ. したがって, 点と直線のインシデンスすなわち, 含むという関係の個数を計算して, $(n+1)(n^2+n+1)=m(1+mn)$ を得る. なぜならば n^2+n+1 個の直線が存在して, そのおのおのは $n+1$ 個の点を含み, 一方において $1+mn$ 個の点が存在してそのおのおのは m 個の直線に含まれるからである. したがって $m=n+1$ であり性質（2),（4）が成り立つ. 次に（6）を示す. 与えられた1直線 L 上の任意の1点 P は n 個の L と異なる直線の上にある. したがって, L は $n(n+1)=n^2+n$ 個の L と異なる直線と交わる. 直線はこれら全部でつきていたから（6）が成り立つ. したがって（1),（3),（5）から, （2),（4),（6）が導かれることが分かった. 双対的に（2),（4),（6）から（1),（3),（5）が容易に導かれる. 証終.

系 20.8.1. 有限 Veblen-Wedderburn 系において, 定理 20.4.6 の条件

（4）（すなわち，$r \neq s$ ならば，$xr = xs + t$ はただ一つの解を持つ）は他の条件から導かれる．

なぜならば，定理 20.4.6 の条件（4）を用いることなしに，その Veblen-Wedderburn 系を座標環とする点と直線の系がこの § のはじめに挙げた性質（1），（3），（5）を満たすことを示せるからである．

各自然数 n に対して，位数 n の有限平面が存在するとは限らない．もし Euler の予想が正しければ，$n \equiv 2 \pmod 4$，$n \neq 2$ のとき，位数 n の有限平面は存在しない．特に位数 6 の有限平面が存在しないことは 1900 年に，Tarry [1] により，試行錯誤の方法で示された．各素数巾 $n = p^r$ に対しては，体 $GF(p^r)$ が存在するから定理 20.5.5 により，位数 p^r のデザルグ平面が存在する．また，位数 p^{2r} の Hall 系が存在し，位数 4 の場合を除けば，これらは非デザルグ平面を作る．また Albert [1] は奇素数 p と $r > 2$ に対して，位数 p^r の非結合的な可逆環（division ring）を構成した．定理 20.4.6 により，これらの可逆環を用いることにより位数 p^r の非デザルグ平面が構成される．ここでは簡単のため，奇素数 p と奇数 $r > 1$ に対して位数 p^r の非結合的可逆代数（non-associative division algebra）を Albert にしたがって構成する．

定理 20.8.2.（Albert）． p を奇素数，r を奇数で，$r > 1$ とする．このとき，$GF(p^r)$ から p^r 個の元からなる非結合的な可逆代数 D を作ることができる．

証：$GF(p^r)$ の元達に対して次のように新しい積 (x, y) を定義する．

(20.8.1) $$(x, y) = \tfrac{1}{2}(xy^p + x^p y).$$

$x \to x^p$ は $GF(p^r)$ の自己同型であるから積 (x, y) が分配律を満たすことは容易に示される．次に $x \neq 0$，$y \neq 0$ ならば $(x, y) \neq 0$ であることを示す．もし $x \neq 0$，$y \neq 0$ かつ，$(x, y) = 0$ が成り立っていると仮定すれば，

(20.8.2) $$xy^p = -x^p y$$

したがって

(20.8.3) $$y^{p-1} = -x^{p-1}$$

である．r，p が共に奇数であることから，$m = (p^r - 1)/p - 1$ も奇数である．

そこで (20.8.3) をm乗すると，

(20.8.4)
$$1=y^{p^r-1}=-x^{p^r-1}=-1$$

であるから，これは $p\neq 2$ であることに矛盾する．したがって $x\neq 0$, $y\neq 0$ ならば $(x, y)\neq 0$ である．ところで，我々の考えているこの代数系は有限個の元からなりしかも零因子を持たないことから，これは準群 (quasi-group) でなければならない．したがって $x\neq 0$ が与えられたとき，

(20.8.5)
$$x=(u, 1)=\tfrac{1}{2}(u+u^p)$$

を満たすような $u\neq 0$ が一意的に存在する．したがって，$GF(p^r)$ からこの代数系の上への1対1の写像αが，

(20.8.6)
$$u=x\alpha$$

により定義される．

次に，$GF(p^r)$ に，加法は通常の加法，乗法 $x\circ y$ を

(20.8.7)
$$x\circ y=(x\alpha, y\alpha)$$

と定義した新しい代数系Dを考える．$GF(p^r)$ の単位元1はDにおいても単位元である．なぜならば，

(20.8.8)
$$x\circ 1=1\circ x=x^4$$

が容易に示される．このようにして可逆環Dが作られたわけである．このときDにおける乗法は可換であるが，結合的でない．Albert は F_p に含まれないある元の巾が結合的でないことを示したのである．

ここで示したのと同様な方法により，位数 p^r (p は奇素数，$r\geqq 2$) および位数 2^r (r は偶数で $r\geqq 2$) の可逆環が構成される．そのことから，その位数の非デザルグ平面の存在が示される．一方，位数2, 3, 4, 5, 7の平面はデザルグ平面に限ることが証明されている．また，この他にも後で述べる Hughes 平面をはじめとして，幾つかの非デザルグ平面が知られている．しかし位数が素数巾でないような平面は知られていない．

位数6の平面が存在しないという Tarry による結果を除けば，平面の位数に関する制限は，1949年の Bruck-Ryser [1] による次の結果が現われるまで，何も知られていなかった．

定理 20.8.3. $n\equiv 1, 2 \pmod 4$ でかつnが，$n=a^2+b^2$ (a, bは整数) と表わせないときには位数nの有限平面は存在しない．

証：ここで与える証明は，Chowla-Ryser [1] における方法を用いて，もとの証明を改良したものである．$N=n^2+n+1$ と置く．変数 x_i, $i=1, 2, \cdots, N$ が位数nの平面π上の各点 P_i, $i=1, 2, \cdots, N$ に対して定められているとする．また，πの直線達を L_j, $j=1, 2, \cdots, N$ で表わす．このとき，次のようにしてインシデンス数 a_{ij} ($i, j=1, 2, \cdots, N$) を定める．

(20.8.9) $$a_{ij}=1, \quad P_i\in L_j \text{ のとき．}$$
$$a_{ij}=0, \quad P_i\notin L_j \text{ のとき．}$$

そこでπのインシデンス行列Aを

(20.8.10) $$A=(a_{ij}), \quad i, j=1, 2, \cdots, N$$

で定義する．このとき，インシデンス行列Aが関係

(20.8.11) $$A\cdot A^T=A^T\cdot A=nI+S$$

を満たすことを以下で証明する．ここでIは単位行列，Sは各要素が1の行列を表わす．

$A\cdot A^T=C$, $C=(c_{rs})$ と置けば

(20.8.12) $$c_{rs}=\sum_{j=1}^{N} a_{rj}a_{sj}$$

である．このとき，$c_{rr}=n+1$ である．なぜならば P_r はちょうど $n+1$ 個の直線上にあり，a_{rj}, $j=1, \cdots, N$ のうちちょうど $n+1$ 個が1で他は0であるからである．また，$r\neq s$ のとき $c_{rs}=1$ である．なぜならば $a_{rj}a_{sj}\neq 0$ であるためには $a_{rj}=1$, $a_{sj}=1$ が共に成り立たねばならないが $a_{rj}=a_{sj}=1$ であることは直線 L_j が P_r と P_s を共に含むことであるからである．したがって以上をまとめれば，$c_{rr}=n+1$, $c_{rs}=1 (r\neq s)$ で $A\cdot A^T=nI+S$ が得られる．また，双対的な論法により，$A^T\cdot A=nI+S$ も得られる．

関係 $A\cdot A^T=nI+S$ を二次形式を用いて表わすこともできる．各直線 L_i に対して一つの一次形式を定める．この一次形式を同じく L_i で表わしてもそれほど混乱の心配はないであろう．

(20.8.13)
$$L_j=\sum_{i=1}^{n} a_{ij}x_i,\quad j=1,\cdots,N$$

とするとき，

(20.8.14)
$$L_1^2+\cdots+L_N^2=n(x_1^2+\cdots+x_N^2)+(x_1+\cdots+x_N)^2$$

が成り立つ．なぜならば，L_j，$j=1,\cdots,N$ において各 x_r は係数 1 でちょうど $n+1$ 回現われ（各点はちょうど $n+1$ 個の直線に含まれるから），また，$2x_rx_s$ という項は，$L_1^2+\cdots+L_N^2$ においてただ一回のみ現われる（P_r と P_s を含む直線はただ一つだから）からである．さて，$n\equiv1,2 \pmod 4$ という仮定から，$N=n^2+n+1\equiv3 \pmod 4$ である．また，(20.8.14) を書き直せば，

(20.8.15)
$$L_1^2+\cdots+L_N^2=n\left(x_2+\frac{x_1}{n}\right)^2+\cdots+n\left(x_N+\frac{x_1}{n}\right)^2+(x_2+\cdots+x_N)^2$$

が得られる．次に (20.18.15) の変数を変換して，

(20.8.16)
$$y_1=x_1+\cdots+x_N,\quad y_2=x_2+\frac{x_1}{n},\ \cdots,\ y_N=x_N+\frac{x_1}{n}$$

と置く．このとき，各 x_i は y_j 達の有理係数の 1 次結合で表わされる．さらに (20.8.15) を書き直して，

(20.8.17)
$$L_1^2+\cdots+L_N^2=y_1^2+ny_2^2+ny_3^2+\cdots+ny_N^2$$

を得る．Lagrange の定理によれば，任意の正の整数は 4 つの平方数の和で表わされる．これに関しては，Hardy-Wright の "Theory of Numbers" [1], p. 300 を参照のこと．

(20.8.18)
$$n=a_1^2+a_2^2+a_3^2+a_4^2$$

と置けば，Lagrange のよく知られた恒等式により，

(20.8.19)
$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2)&(y_i^2+y_{i+1}^2+y_{i+2}^2+y_{i+3}^2)\\ &=(a_1y_i+a_2y_{i+1}+a_3y_{i+2}+a_4y_{i+3})^2\\ &\quad+(a_1y_{i+1}-a_2y_i+a_3y_{i+3}-a_4y_{i+2})^2\\ &\quad+(a_1y_{i+2}-a_3y_i+a_4y_{i+1}-a_2y_{i+3})^2\\ &\quad+(a_1y_{i+3}-a_4y_i+a_2y_{i+2}-a_3y_{i+1})^2\\ &=z_i^2+z_{i+1}^2+z_{i+2}^2+z_{i+3}^2\end{aligned}$$

を得る．ここで，z_i, z_{i+1}, z_{i+2}, z_{i+3} は，y_i, y_{i+1}, y_{i+2}, y_{i+3} の有理係数の一次結合で表わされていることに注意しよう．$N\equiv 3 \pmod 4$ であったから，(20.8.18), (20.8.19) を (20.8.17) に適用して

(20.8.20) $$L_1^2+\cdots+L_N^2=z_1^2+z_2^2+\cdots+z_{N-2}^2+n(z_{N-1}^2+z_N^2)$$

が得られる．各 L_j, $j=1,\cdots,N$ が x_i 達の有理係数の（実際には整係数の）一次形式であり，また y_j 達の有理係数一次結合であり，さらには独立変数 z_j 達の有理係数一次結合である．(20.8.20) は z_j 達に関する恒等式であるから，z_j の幾つかのものを他のものの一次結合で表わしたものに入れ換えても変化しない．そこで (20.8.20) において

(20.8.21) $$L_1=b_1z_1+\cdots+b_Nz_N$$

であったとすれば，$b_1\neq 1$ のとき，$L_1=z_1$, $b_1=1$ のとき，$L_1=-z_1$ と置くことにする．そこで，これ等のいずれかを用いて，z_1 を $z_2,\cdots,z_N$ の有理係数一次結合で表わすことができ，また，$L_1^2=z_1^2$ が成り立つ．したがって，

(20.8.22) $$L_2^2+\cdots+L_N^2=z_2^2+\cdots+z_{N-2}^2+n(z_{N-1}^2+z_N^2)$$

を得る．したがって，以下順々に，$L_2=\pm z_2,\cdots,L_{N-2}=\pm z_{N-2}$ と置くことにより，

(20.8.23) $$L_{N-1}^2+L_N^2=n(z_{N-1}^2+z_N^2)$$

を得る．ここで L_{N-1}, L_{N-2} は 2 つの独立変数 z_{N-1}, z_N に関する有理係数一次形式である．いま，z_{N-1}, z_N を L_{N-1}, L_N における係数の分母に現われるものの倍数とすれば，(20.8.23) はすべての係数が整数であるような関係式となる．ところが整数 n はある 2 つの平方数の和をある 2 つの平方数の和で割ったものであるから，Hardy-Wright [1] p. 366 における数論でよく知られた定理により，n はそれ自身 2 つの平方数の和で表わされる．したがって，$n=a^2+b^2$ (a, b 整数) と表わされる．証終．

この定理の一部分に対して，その逆が成り立つことを次に示す．

定理 20.8.4. $n\equiv 0, 3 \pmod 4$ または $n\equiv 1, 2 \pmod 4$ かつ $n=a^2+b^2$ ならば，$x_1,\cdots,x_N$ に関する有理係数一次形式 L_j, $j=1,\cdots,N$ が存在して，

$L_1^2+\cdots+L_N^2=n(x_1^2+\cdots+x_N^2)+(x_1+\cdots+x_N)^2$ を満たす．さらに，各要素が有理数からなる $N\times N$ 行列 A で $A\cdot A^T=A^T\cdot A=nI+S$ を満たすものが存在する．

証：もし $n\equiv 0, 3 \pmod 4$ であれば (20.8.18), (20.8.19) を (20.8.17) に代入して

(20.8.25)
$$L_1^2+\cdots+L_N^2=z_1^2+\cdots+z_N^2$$

を得る．このとき，$L_i=z_i$ と置けば，これらが定理の条件を満足する．もし $n\equiv 1, 2 \pmod 4$, $n=a^2+b^2$ であれば，恒等式

(20.8.26)
$$(a^2+b^2)(y_i^2+y_{i+1}^2)=(ay_i+by_{i+1})^2+(by_i-ay_{i+1})^2$$
$$=z_i^2+z_{i+1}^2$$

を (20.8.19) の代わりに (20.8.17) に代入すれば，同様にして式 (20.8.25) を得る．一方，

(20.8.27)
$$L_j=\sum_i b_{ij}x_i,\quad j=1,\cdots,N$$

が定理の条件を満たす一次形式であるとき，$A=(b_{ij})$, $i, j=1,\cdots,N$ と置くと

(20.8.28)
$$A\cdot A^T=nI+S$$

が満たされる．ただし一般には $A^T\cdot A=nI+S$ は成り立たない．定理の仮定の下に，有理係数の行列 A で，$A\cdot A^T=nI+S$ と $A^T\cdot A=nI+S$ を同時に満たすものがあることを示すことは，かなりむずかしい．しかしこのことは Hall-Ryser [1] により示された．またそこではさらに詳しい結果が得られている．

20.9. 有限平面における共線変換

平面 π の共線変換 α が2点を固定すれば，α はその2点を結ぶ直線も固定する．同様に α が2直線を固定すれば，α はその交点も固定する．したがって，もし α が quadrilateral を固定すれば，α は部分平面を固定する．次の定理で部分平面の位数がどのようになるかを記述する．

定理 20.9.1. (**Bruck**). 位数 n の平面 π が位数 m の部分平面 π^* を持てば，

$n=m^2$ または $n>m^2+m$ である．

証：L を部分平面 π^* の直線，P を π^* に含まれない L 上の点とする．このとき，π^* 上の点のうち $m+1$ 個はLの点で他の m^2 個の点は L 上にない．P とそのL上にない m^2 個の点をそれぞれ結ぶと，P を含む m^2 個の直線が得られ，しかもそれらはすべて異なっている．なぜならば，それらのうちの２つが同一の直線Kであるとすれば，Kは π^* の２つの異なる点を含み π^* の直線と考えられ，KとLの交点がPであり，Pが π^* の点でないという仮定に反するからである．したがって，Pを通る直線は，LとPと π^* の点を結ぶ m^2 個のLと異なる直線とで，少なくとも m^2+1 個は存在する．一方Pを通る直線の個数は $n+1$ 個であるから $n\geqq m^2$ である．もし $n\neq m^2$ とすれば，Pを通り，π^* のいかなる点も含まないような直線 L_1 がさらにもう一つ存在する．さて次に，m^2+m+1 個の π^* の直線達と L_1 との交点について考えよう．もしこれらの交点のうちの２つが同一であれば，その点は π^* の点となり仮定に反する．したがって L_1 は少なくとも m^2+m+1 個の点を含み，$n\geqq m^2+m$ が得られる．証終．

平面の点と直線の部分集合の組Sで，Sの２点に対しては，それらを結ぶ直線をSの中に含み，かつSに含まれる２直線の交点をSの中に含むようなものについて考えよう．

もしSが，“一般の位置にある”４点を含めば，Sは部分平面である．部分平面にならない部分集合Sのことを**縮退部分平面**（degenerate subplane）とよぶことにする．それらは，

1）空集合．

2）一点PとPを通る一つまたはいくつかの直線．

3）一直線LとLに含まれる一つまたはいくつかの点．

4）一点PとPを通らない一直線．

5）三角形の頂点と辺．

6）一直線L，L上の一点P，L上の１つまたは幾つかの点，およびPを通

る1つまたは幾つかの直線.

7) 3点またはそれ以上を含む一直線L, L上にない一点P, およびPとL上の点を結ぶ直線全部.

のいずれかである.

共線変換αは, 点の集合の上の置換として働き, また直線の集合の上の置換としても働く. αから導かれる点, 直線の集合の置換をそれぞれP, Qで表わすと, P, Qは$N\times N$行列で表わされる. $N=n^2+n+1$であり,

(20.9.1) $P=(p_{ij})$, $P_i\alpha=P_j$ のとき $p_{ij}=1$, 他の $p_{ij}=0$

$Q=(q_{ij})$, $Q_i\alpha=Q_j$ のとき $q_{ij}=1$, 他の $q_{ij}=0$

である. $A=(a_{ij})$をπのインシデンス行列とするとき,

(20.9.2) $$P^{-1}AQ=A$$

が得られる. 逆に, (20.9.2)を満たす行列P, Qが存在すれば, それらはπの共線変換を引き起こす.

定理 20.9.2. (**Parker [1]**) 点の集合の上の置換Pと直線の集合上の置換Qは, 置換として相似 (similar) である.

系 20.9.1. (**Baer**). 共線変換で固定される点の個数と直線の個数は等しい.

証:

(20.9.3) $$AA^T=A^TA=nI+S$$

であるから,

(20.9.4) $$(\det A)^2=\det(nI+S)=(n+1)^2n^{N-1}$$

であり, したがってAは非退化 (non-singular) 行列である. したがって, (20.9.2)より

(20.9.5) $$Q=A^{-1}PA$$

が得られ, P, Qは行列として相似である. したがって, 行列P, Qの固有値が同じであることから, 置換P, Qの巡回表示は同じでなければならず, したがって, P, Qは置換として相似である. 特にP, Qの1-cycleの個数, すな

わち P, Q による固定要素の数は等しいから，系の証明も完成した．証終．

定理 20.9.3. (**Parker**) π の共線変換からなるある群 G の，点上の置換群とみての可移域の個数と，直線上の置換群とみての可移域の個数は等しい．

証：群 G の位数を g とする．G を点上への置換群とみたとき G_1, 直線上の置換群とみたとき G_2 と表わせば (20.9.5) により G_1 と G_2 は置換群として同型 (equivalent) である．χ_1, χ_2 をおのおの G_1, G_2 の置換表現の指標とすると，

(20.9.6)
$$\sum_{x\in G}\chi_1(x)=\sum_{x\in G}\chi_2(x)$$

が成り立つ．一方，定理 16.6.13 により，

(20.9.7)
$$\sum_{x\in G}\chi_1(x)=k_1g,\quad \sum_{x\in G}\chi_2(x)=k_2g$$

ここで，k_1, k_2 はおのおの G_1, G_2 の可移域の個数であるから，$k_1=k_2$ が成り立つ．証終．

しかしながら，先の定理 20.9.2 により，G_1 の各元は対応する G_2 の元と置換として相似であったが，一般に G_1 と G_2 は置換群として相似であるとは限らない．たとえば，デザルグ平面において，一点 P_0 を固定する共線変換全体の作る群は，いかなる直線も固定しない．

定理 20.9.4. 位数 $n=p^r$ のデザルグ平面 π の共線変換群の位数は $r(n^2+n+1)(n^2+n)n^2(n-1)^2$ である．

証：π において，その頂点が順序づけられている quadrilateral P_1, P_2, P_3, P_4 のとり方は全部で $(n^2+n+1)(n^2+n)n^2(n-1)^2$ 通りある．なぜならば P_1 として n^2+n+1 個の点から任意に選ぶことができ，P_2 として P_1 と異なる任意の点を，P_3 として直線 P_1P_2 上にない任意の点を，P_4 として P_1P_2, P_1P_3, P_2P_3 のどの直線上にもない任意の点を選べるからである．定理 20.5.5 により，π の共線変換群 G は quadrilateral の集合の上に可移である．G の部分群で quadrilateral X, Y, O, I を固定するものは，座標体 (coordinate field) $GF(p^r)$ の自己同型からなり，§20.6 で注意したように，この位数は r

である．証終．

定理 20.9.5.（Singer [1]）位数 n のデザルグ平面は，点の集合および直線の集合の上に巡回的である位数 $N=n^2+n+1$ の共線変換 α を持つ．

証：$n=p^r$ と置く．π の座標体は $GF(p^r)$ である．π を同次座標（homogeneous coordinate）で表わす．すなわち，1点 P を

(20.9.8)
$$P=(\lambda x_1, \lambda x_2, \lambda x_3)$$

で表わす．ここで，x_1, x_2, x_3 は F の P によって決まる元であり，少なくとも1つは0でない．また λ は F の0でない元全体を動く．同様に，1直線 L は，

(20.9.9)
$$L=[u_1\mu, u_2\mu, u_3\mu]$$

で与えられる．ここで，u_1, u_2, u_3 は F の L によって決まる元であり少なくとも1つは0でない．また μ は F の0でない元全体を動く．$P\in L$ であるための必要十分条件は，

(20.9.10)
$$x_1u_1+x_2u_2+x_3u_3=0$$

で与えられる．F は体であるから，インシデンスの関係（20.9.10）は λ, μ をどのように選んでも同じである．したがって，この同次座標を次のようにして非同次座標と同一視できる．

(20.9.11)
$$\begin{aligned}(\infty)&=(0, \lambda, 0)\\(m)&=(\lambda, \lambda m, 0)\\(a, b)&=(\lambda a, \lambda b, \lambda)\\L_\infty&=[0, 0, \mu]\\(x=c)&=[\mu, 0, -c\mu]\\(y=mx+b)&=[m\mu, -\mu, b\mu].\end{aligned}$$

平面 π の，同次座標による表現と，非同次座標による表現が上の対応により一致することを見るのは容易である．次に，$GF(p^{3r})=F_1$ は，$F=GF(p^r)$ の3次拡大であると考えられ，w を F_1 の原始根とするとき，F_1 の各元は，

(20.9.12)
$$x=x_1+x_2w+x_3w^2,\quad x_i\in F$$

と一意的に表わされる．したがって，もし $x\neq0, \lambda\in F, \lambda\neq0$ であれば，F_1 の

元 λx は π の点 $(\lambda x_1, \lambda x_2, \lambda x_3)$ に対応する．F_1 において，w の位数は $p^{3r}-1=n^3-1$ である．一方，Fの各元は，F_1 における方程式

(20.9.13) $$x^{p^r}=x$$

の解であるから，$x\in F$，$x\neq 0$ ならば，$n=p^r$ に注意して

(20.9.14) $$x^{n-1}=1$$

が成り立つ．

したがって F^* (F の 0 以外の元全体) は，位数 n^3-1 の巡回群 $\{w\}$ の唯一の位数 $n-1$ の部分群である．すなわち，F^* の元は

(20.9.15) $$w^{Ni},\quad N=n^2+n+1,\quad i=0, 1, \cdots, n-2$$

でつくされる．したがって，w^u と w^v が π の同一の点を表わすための必要十分条件は

(20.9.16) $$u\equiv v(\mathrm{mod}\ N)$$

が成り立つことである．したがって，F_1 から F_1 の上への写像

(20.9.17) $$\alpha : x \longrightarrow xw$$

は π の点の集合の上へ位数Nの巡回置換として働く．相異なる 2 点 $P_1=(x_1, x_2, x_3)$，$P_2=(y_1, y_2, y_3)$ を結ぶ直線 P_1P_2 上の点は，

(20.9.18) $$\lambda_1(x_1, x_2, x_3)+\lambda_2(y_1, y_2, y_3)$$
$$=(\lambda_1x_1+\lambda_2y_1, \lambda_1x_2+\lambda_2y_2, \lambda_1x_3+\lambda_2y_3)$$

により与えられる．ここで，λ_1, λ_2 は両方とも 0 と異なるFの元である．したがって，もし $w^i=x_1+x_2w+x_3w^2$，$w^j=y_1+y_2w+y_3w^2$ であれば，P_1P_2 上の点は，

(20.9.19) $$\lambda_1w^i+\lambda_2w^j$$

で与えられる．写像 $\alpha : x\to xw$ は，元 (20.9.19) を

(20.9.20) $$\lambda_1w^{i+1}+\lambda_2w^{j+1}$$

に移す．が，これらの点は，$P_1\alpha$ と $P_2\alpha$ を結ぶ直線上の点である．したがって α は π の共線変換であり，点の集合の上に働く位数Nの巡回置換である．直ちに分かるように，(たとえば定理 20.9.2 により) α は π の直線の集合の上でも，位数Nの巡回置換である．証終．

位数nの平面πにおける共線変換全体からなる群に対して，その位数の上限を，大ざっぱにではあるが，与えることができる．順序づけられた quadrilateral P_1, P_2, P_3, P_4 のGによる像は，たかだか $M=(n^2+n+1)(n^2+n)n^2(n-1)^2$ 個である．指数がM以下の(Gの)部分群 H_1 が P_1, P_2, P_3, P_4 を全体として固定するならば，それらの点から生成される部分平面 π_1 もまた H_1 によって固定される．したがって，もし π_1 の位数が m_1 であれば，H_1 は，π_1 のある直線上にあり，かつ π_1 に含まれないような $n-m_1$ 個の点の上の置換を引き起こす．次に，H_1 における指数 $\leqq n-m_1$ で，4点のうちのある一点を固定するような，部分群 H_2 を考える．この H_2 は π_1 よりも大きい部分平面 π_2（位数を m_2 とする）を固定する．定理 20.9.1により，$m_2 \geqq m_1^2$ が成り立つ．したがって，順々に下がってくる部分群の列 $H_1 \supset H_2 \supset \cdots \supset H_s=1$ が得られる．ここで，H_i は位数 m_i の部分平面を固定し，$m_{i+1} \geqq m$, $[H_i : H_{i-1}] < n$ が成り立っている．したがって $s \leqq \log_2 n$ であり，Gの位数はたかだか $n^s M$ である．知られている非デザルグ平面の共線変換群の位数は同じ位数のデザルグ平面の共線変換群の位数ほど大きくはない．このことが成り立つことはもっともらしい[1]．

次に述べる2つの定理は共線変換群がある意味で大きければ，その平面はデザルグ平面であることを主張する．

定理 20.9.6.（**Gleason [1]**）平面πの直線Lとその上の点Pからなる任意の組に対して，その相応（elation）群，$G(P, L)$ が単位元以外の元を含めば，π はデザルグ平面である．

証：定理 20.4.3により，L上の相異なる2点 P_1, P_2 に対する相応群 $G(P_1, L)$, $G(P_2, L)$ が共に単位元以外の元を含めば，Lを軸とする相応の全体は，単位元を除いた各元の位数がある同一の素数 p であるようなアーベル群を作る．この定理 20.4.3の双対を考えれば，もしPを通る相異なる2直線 L_1, L_2 に対して，$G(P, L_1)$ と $G(P, L_2)$ が共に，単位元以外の元を含めば，Pを中

1) まだ証明はされていない．

心とする相応の全体は単位元を除いた各元の位数がある同一の素数巾であるようなアーベル群を作る．したがって，定理の仮定により各相応群 $G(P, L)$ は位数 p または p 巾の初等アーベル群である．

補題 20.9.1. Hを有限集合 S 上に働く置換群とし，各 $x \in S$ に対して，H の元で，x のみを固定し他の S の元をすべて動かし，位数がある定まった x によらない素数 p であるようなものが存在すると仮定する．このとき H は S 上可移である．

証：S_1 を H のある可移域とする．$x \in S_1$ に対して，x を固定し，他の元を長さ p の巡回置換により移すような，位数 p の H の元が存在する．したがって，S_1 の元の個数 $\equiv 1 \pmod p$ であり，他の可移域 S_2 の元の個数は p の倍数である．しかし，$y \in S_2$ なる元に対して，同じ論法を用いれば，S_1 の元の個数は p の倍数になり矛盾が生じる．したがって H の可移域はただ一つである．すなわち H は可移である．証終．

補題 20.9.2. 有限平面のある 1 つの直線 L に対して，相応群 $G(P_i, L)$ の位数が各 $P_i \in L$ に対して一定の値 $h>1$ であると仮定する．このとき，π は L に関する移行平面である．

証：π の位数を n とする．$n+1$ 個の群 $G(P_i, L)$ のうち，どの 2 つをとっても，それらは単位元以外に共通な元を持たず，移行群 $T(L)$ を生成する．したがって，$T(L)$ の位数は，$t=(n+1)(h-1)+1$ である．L 上にない点を固定するような $T(L)$ の元は単位元に限るから，$T(L)$ によって残りの n^2 個の点を可移域に分けたとき，各可移域に含まれる元の個数はある一定の値 t に等しい．したがって，

(20.9.21)　$$n^2 = tm = [(n+1)(h-1)+1]m$$

が成り立つ．$h>1$ であるから $m<n$ である．一方 (20.9.21) を $\bmod n+1$ で考えると

(20.9.22)　$$n^2 \equiv 1 \equiv m \pmod{n+1}$$

が得られる．したがって，$m<n$ であるから，$m=1$，したがって $t=n^2$ であり，$T(L)$ は π の L 上にない n^2 個の点の上に可移である．すなわち，π は L に関する移行平面である．

さて定理の証明に移る．π から1つの直線 L を選び固定する．各点 $P\in L$ に対して，相応群 $G(P, M)$（ここで，M は P を通り，直線 L と相異なる直線とする）は P を固定し，L をそれ自身に移し，L 上の P と異なる点をすべて動かすような位数 p の元を持つ．したがって，補題20.9.1により，L を固定する共線変換全体の作る群 $G(L)$ は，L の点の集合の上に可移である．したがって，各 $P_i\in L$ に対して，$G(P_i, L)$ が $n+1$ 個できるが，それらは $G(L)$ で互いに共役であり，それらの群の位数はすべて同一（$=h$）である．したがって補題20.9.2によって，π は L に関する移行平面である．L は π の任意の直線でよかったから，π は任意の直線に関して移行平面である．したがって，定理20.6.2によって，π は交代可逆環により座標づけられる．定理20.6.2で見たように有限交代可逆環は体であるから，π はデザルグ平面である．証終．

Gleason [1] は，この定理を用いて，有限 Fano 平面を研究した．Fano 図形（Fano configuration）とは，位数2の射影平面を作っている7点と7直線からなる図形をいう．平面が Fano 平面であるとは，各 quadrilateral の各点を互いに結ぶ直線の交点達が同一直線上にあることをいう．言い換えれば，各四辺形が Fano 平面を生成することをいう．Gleason は有限 Fano 平面はすべて，デザルグ平面であり，それらは体 $GF(2^r)$ 上の平面であることを示した．これは非常に興味深い結果ではあるが，紙面の都合もあり省略することにする．

位数2の共線変換を対合（involution）とよぶ．

定理 20.9.7.（Baer）．α が位数 n の射影平面の対合であれば，（1）$n=m^2$ であり，α により固定される点と直線は位数 m の部分平面を作る，または（2）α は中心共線変換である，のいずれかが成り立つ．特に（2）が起こる

場合には，nが奇数ならαはホモロジー，nが偶数ならαは相応である.

証：まず，任意の点Pに対して，点Pを通りαにより固定されるような直線が存在することを示す．もしPがαにより固定されなければ，$P\alpha \neq P$ であり，直線 $PP\alpha$ はPを含み，しかもαで固定される。次に，もしPがαで固定されれば，Pと他の任意の点Qを結んだ直線 $PQ=L$ がαにより固定されることを示そう．もし PQ がαで固定されなければ，$Q\alpha \neq Q$ で $Q\alpha \notin PQ$ が成り立ち，$L\alpha = PQ\alpha$ である．したがって，RをPともQとも異なるL上の点としたとき，$R\alpha \in L\alpha$ である．このとき，αは $Q\alpha R$ と $QR\alpha$ とを入れ換える．したがってこの2直線の交点Sはαによって固定され，しかもSはPと異なる．したがって，直線 PS はPを通りしかもαによって固定される．双対性によって，任意の直線はαにより固定される点を含む.

αにより固定されるような2点を結ぶ直線もαで固定される．またαにより固定される2直線の交点もαで固定される．したがって，各点がαにより固定される，“一般の位置にある” 4点が存在すれば，αによって固定される点と直線の集合は，πの部分平面π_1を作る．さて，このような場合が起こったと仮定しよう．π_1の位数をmとすれば，定理20.9.1により $n \geqslant m^2$ が成り立つが，そこでの証明を見れば分かるように，もし $n > m^2$ であれば，πの直線でπ_1の点を1つも含まないものが存在することが分かる．しかし．先に述べたようにπの任意の直線はαにより固定される点を含むから $n > m^2$ の場合は起こりえない．したがって $n = m^2$ であり，定理における（1）の場合が起こる.

次に，各点がαにより固定されるような一般の位置にある4点が存在しないと仮定する．このとき，αにより固定される点全体はどのような図形を作るであろうか？ まず，αにより固定される3点を含む直線が存在することを示そう．直線L_1はある（αによる）固定点P_1を含む．P_1を通らない直線L_2を1つ選べば，L_2も固定点 $P_2 \neq P_1$ を含む．したがって，P_1とP_2を結ぶ直線Lは固定される．L上にあるP_1とP_2と異なる第三の点Qを1つ選ぶ．もし

Qが固定されれば，Lは求める直線である．もしQが固定されなければ，Qを通りLと異なる直線 L_3 を選ぶ．Lもある固定点 P_3 を持つ．このとき３つの固定点 P_1, P_2, P_3 は三角形を作る．次に P_1, P_2, P_3 のいずれの点も通らない直線 L_4 を考えれば，L_4 もまた固定点 L_4 を含む．もし P_4 が３つの直線 P_1P_2, P_1P_3, P_2P_3 のいずれにも含まれなければ，４点 P_1, P_2, P_3, P_4 は一般の位置にあり仮定に反する．したがって３つの固定点を含むような直線が存在する．

いま，直線Lが３つの固定点 P_1, P_2, P_3 を含むとする．L上にない固定点が２つ以上あれば，一般の位置にある４つの固定点が存在するから仮定に反する．したがって，L上にない固定点は存在してもたかだか１つである．L上の任意の点Rに対して，Rを通り，Lと異なる直線Kが存在する．もしL上にない固定点Pが存在するならば，Kは PR とも異なるようにとっておける．Kは固定点を含むが，その固定点はL上になければならず，したがってRである．したがってL上の各点はいずれも α によって固定される．したがって α はLを軸とする中心共線変換であり，定理における（２）の場合が起こる．L上にない π の点の個数は n^2 で，α は位数２だから，もしnが奇数ならば，α はL上にない一点を固定するのでホモロジーであり，もしnが偶数ならば，α はL上にない偶数個の点を固定するので，もしαがL上にない固定点を持てばその個数は２以上でなければならない，したがってそのようなことは起こらないから，α は相応である．証終．

次の定理は，Ostrom [1] の定理を少し改良したものである．Ostrom はnが奇数という仮定を課していた．

定理 20.9.8.（Ostrom）. 有限射影平面 π の位数nが平方数でなく，さらに π の共線変換群が π の点の集合の上に２重可移であれば，π はデザルグ平面である．

証：π の共線変換群Gは仮定により，π の $N=n^2+n+1$ 個の点の集合の上に２重可移である．したがって $N(N-1)$ はGの位数を割るから，Gは位数２の元，すなわち対合 α を含む．nが平方数でないから，定理 20.9.7 により，

nが偶数であればαはホモロジーであり，nが奇数であればαは相応である.

補題 20.9.3. Gは相応を含む.

証：nが偶数ならば，対合は相応であるから明らか．したがって，以下nは奇数と仮定して良い．対合αを1つとれば，αはホモロジーである．その中心をP，軸をLとする．Lの点AとL上にない点 $A_1 \neq P$ を任意にとれば，PをPに移し，Aを A_1 に移すGの元σが存在する．このとき，$\beta=\sigma^{-1}\alpha\sigma$ は中心がP，軸が A_1 を通るある直線K（したがってLと異なる）である対合である．$\alpha\beta$ はPを通るすべての直線を固定するから中心共線変換である．もし，$\rho=\alpha\beta$ がPを通らない直線Tを固定すれば，$T_1=T\alpha$ と置いたときβはTとT_1を入れ換える．したがって，$T \neq T_1$ ならば，ρはT, T_1を固定するから，定理20.4.1により $\rho=1$ であり，$\alpha=\beta$ である．しかし対合αとβの軸は異なるからこれは矛盾である．したがって，ρはPを通らない直線は固定しない．したがって，ρは相応である．証終.

さて次に中心がP，軸がLの相応ρを考えよう．RをPと異なるLの任意の点とすれば，Gの元σでPとRを入れ換えるものが存在する．したがってσはLを固定する．それゆえ群 $G(L)$（Lを固定する共線変換全体の作る群）はL上の点の集合の上に可移である．したがって，Lの各点Rに対して相応群$G(R, L)$ は同じ位数hを持つ．ところでρが $G(P, L)$ に含まれていたから実際 $h>1$ である．したがって補題20.9.2により，πは軸Lに関して移行平面である．一方，Gは点の集合の上に二重可移であるから，Gの適当な元を選ぶことにより，L上の任意の2点は，他の任意の直線K上の任意の2点に移すことができる．したがってπは軸Kに関しても移行平面である．すなわちπはMoufang 平面である．したがって，定理20.9.6により，πはデザルグ平面である．証終.

A. Wagner による未発表[1]の論文によれば，定理20.9.8はnに関する制限

---

1) Ostrom and Wagner, On projective and affine planes with transitive collineation groups, Math. Z. 71, (1959).

なしに成り立つ.

D. R. Hughes [3] により与えられた，一般化されたインデンス行列について考えよう．まず初めに，以下で用いる記号をまとめておこう．

π：位数 n の射影平面

G：π の共線変換からなるような1つの群．Gの位数を g で表わす．

G^*：Z上（または標数がGの位数を割らないような体上）の群環．

w：Gをπの点の集合の上の置換群とみたときの可移域の個数.（定理 20. 9. 3 によりwはGをπの直線上の置換群と見た時の可移域の個数にもなっている.）

$P_i, i=1, \cdots, w$：点の集合の作る第 i 番目の可移域から選んだ代表系.

$L_i, i=1, \cdots, w$：直線の集合の作る第 i 番目の可移域から選んだ代表系.

H_i：1点 P_i を固定するGの元全体の作る部分群. H_i の位数を h_i で表わす.

T_j：1直線 L_j を固定するGの元全体の作る部分群．T_j の位数を t_j で表わす.

$D_{ij}=\{x \mid x\in G,\ P_ix\in L_j\}$：$D_{ij}$ に含まれるGの元の個数を d_{ij} で表わす.

$$\delta_{ij}=\sum x,\quad x\in D_{ij}$$

$$\delta^*_{ij}=\sum x^{-1},\quad x\in D_{ij}$$

$$D=(\delta_{ij}),\quad i, j=1, \cdots, w\ (G^*\ \text{上の行列})$$

$$(20.9.23)\qquad D'=(\delta^*_{ij})^T,\quad i, j=1, \cdots, w\ (G^*\ \text{上の行列})$$

$$\rho_i=\sum x,\quad x\in H_i,\quad i=1, \cdots, w$$

$$\tau_j=\sum x,\quad x\in T_j,\quad j=1, \cdots, w$$

$$\gamma=\sum x,\quad x\in G$$

$S=$各要素ですべて γ である $w\times w$ 行列.

さらに，次のような対角行列を用いる.

$$C_1=\text{diag.}\,(h_1^{-1}, h_2^{-1}, \cdots, h_w^{-1})$$

$$(20.9.24)\qquad C_2=\text{diag.}\,(t_1^{-1}, t_2^{-1}, \cdots, t_w^{-1})$$

$$P=\text{diag.}\,(\rho_1, \rho_2, \cdots, \rho_w)$$

$$L=\text{diag.}\,(\tau_1, \tau_2, \cdots, \tau_w)$$

もし，Dについての（するわち，各 D_{ij} に含まれる G の元についての）情

報が完全にわかれば，π のインシデンスは完全に決まる．なぜならば，π の各点は適当な $i(i=1,\cdots,w)$ と $u\in G$ を選ぶことにより P_iu と表わされ，同様に各直線は L_iv と表わされ，$P_iu\in L_jv$ が $P_iuv^{-1}\in L_j$，すなわち $uv^{-1}\in D_{ij}$ と同値になるからである．特に，Gが単位群のときは，Dは通常のインシデンス行列Aに他ならない．

定理 20.9.9. 位数 n の平面 π と π の共線変換の作る位数 g の群Gが与えられているとする．このとき，行列Dは次の関係を満たす．

$$DC_2D'=nP+S$$
(20.9.25)
$$D'C_1D=nL+S$$
$$DC_2S=(n+1)S$$
$$SC_1D=(n+1)S$$

証：まず1番上の式を証明する．$DC_2D'=U=(u_{r,s})r, s=1,\cdots,w$ と置いたとき，Uの対角成分は，

(20.9.26)
$$u_{rr}=\sum_{j=1}^{w}\frac{\delta_{rj}\delta^*{}_{rj}}{t_j}$$

で与えられ，この式（20.9.26）の右辺の j 番目の項は

(20.9.27)
$$\sum\frac{xy^{-1}}{t_j},\quad x\in D_{rj},\quad y\in D_{rj}$$

である．$x\in D_{rj}$ に対して，剰余類 H_rxT_j は D_{rj} に含まれることに注意しよう．Gを H_r による左剰余類の和に分ける．すなわち，

(20.9.28)
$$G=H_r+H_rx_2+\cdots+H_rx_{v_r},\quad v_rh_r=g.$$

このとき，$h\in H_r$ に対して，方程式 $xy^{-1}=h$（すなわち $x=hy$）は任意の $y\in D_{rj}$ に対して解 $x\in D_{rj}$ を持つ．なぜならば，任意の $y\in D_{rj}$ に対して $H_ry\subseteq D_{rj}$ だからである．したがって与えられた $h\in H_r$ に対して，$xy^{-1}=h$ を満たす $x, y\in D_{rj}$ の組は d_{rj} 個ある．したがって，式（20.9.26）において，h の係数は $\sum_j d_{rj}/t_j$ である．一方，d_{rj} は $P_rx\in L_j$（すなわち，$P_r\in L_jx^{-1}$）となる x の個数であり，L_jx^{-1}, $x\in D_{rj}$ なる形の相異なる直線の個数は d_{rj}/t_j である．一方 P_r を通る直線は全部で $n+1$ 個あるから

(20.9.29)
$$\sum_j \frac{d_{rj}}{t_j}=n+1$$

が成り立つ．したがって，(20.9.26) における，$h\in H_r$ の係数は $n+1$ である．

次に，$xy^{-1}=z$, $z\notin H_r$ の解 x, y の個数を調べる．点 P_r と P_{rz} は相異なるから，それらは一意的に決まる直線 L_mv 上にある．ここで m と剰余類 T_mv は一意的に定まる．もし，ある j に対して $x\in D_{rj}$, $y\in D_{rj}$ であれば，P_ry および $P_rzy=P_rx$ はいずれも L_mvy に含まれる．しかし，$P_sy\in L_j$, $P_rx\in L_j$, $P_rx\neq P_sy$ であるから，$L_mvy=L_j$ である．したがって $j=m$, $vy\in T_m$ である．したがって (20.9.26) において，z は $j=m$ のときのみ現われる．そのとき $x\in D_{rm}$, $y\in D_{rm}$ である．一方，$y\in D_{rm}$ に対して，$x=zy\in D_{rm}$ が成り立てば，$P_ry\in L_m$, $P_rzy\in L_m$ であり，したがって $P_ryP_rzy=L_m$ である．また $P_ryP_rzy=(P_rP_rz)y=L_mvy$ であり，$L_m=L_mvy$ が成り立つ．したがってこのとき $y^{-1}\in T_mv$ である．このような y はちょうど t_m 個ある．また逆に，$y^{-1}\in T_mv$ なる y に対して，$x=zy\in D_{rm}$ が成り立つ．したがって，(20.9.26) において $z\notin H_r$ の係数は $t_m/t_m=1$ である．以上のように，(20.9.26) における $h\in H_r$ の係数は $n+1$, $z\notin H_r$ の係数は 1 である．したがって，(20.9.25) の第1番目の等式が，主対角成分に関するところまで証明された．

次に，$U=DC_2D'$ の対角成分でないものは，

(20.9.30)
$$u_{rs}=\sum_{j=1}^{m}\frac{\delta_{rj}\delta^*_{sj}}{t_j},\quad r\neq s$$

で与えられる．この式 (20.9.30) の右辺の j 番目の項は

(20.9.31)
$$\sum\frac{xy^{-1}}{t_j},\quad x\in D_{rj},\quad y\in D_{sj}$$

で与えられる．このとき，任意の $z\in G$ に対して，P_rz は P_s と異なるから P_rz, P_s は一意的に定まるある直線 L_mv 上にある．ここで，m と T_mv は一意的に決まる．このとき，ある j に対して $xy^{-1}=z$ なる $x\in D_{rj}$ と $y\in D_{sj}$ が存在するとすれば，$P_rx=P_rzy$ であり，P_sy は L_mvy に含まれる．一方，$P_rx\neq P_sy$ であり，両方とも L_j に含まれるから $L_mvy=L_j$ が成り立つ．し

たがって $j=m$ であり，$L_j y^{-1}=L_m v=P_r z P_s$，$y^{-1}\in T_m v$ である．このような y はちょうど t_m 個ある．逆に $y^{-1}\in T_m v$ ならば $L_m v y=L_m$ かつ $P_r z y \in L_m$，したがって，$x=zy\in D_{rm}$ である．したがって，u_{rs} に現われる z の係数は $t_m/t_m=1$ である．したがって，$u_{rs}=\sum z$，$z\in G$，すなわち $u_{rs}=\gamma$ が成り立つ．以上により，(20.9.25) の1番目の等式が証明された．

(20.9.25) の2番目の等式は1番目の等式に対する双対であり，同様な方法で証明できる．

次に $DC_2S=V=(v_{rs})$ を計算する．まず，

(20.9.32)
$$v_{rs}=\sum_j \frac{\delta_{rj}}{t_j}\gamma=\sum_j \frac{d_{rj}}{t_j}\gamma$$

である．(20.9.29) によりこれは $(n+1)\gamma$ に等しい．したがって3番目の等式が証明された．4番目の等式は3番目の等式に対する双対であり，同様の方法で証明される．証終．

関係 (20.9.5) から出発して，Hughes は平面における共線変換がかなり制限されることを示した．すなわち，次に述べる定理である．この証明には (Bruck-Ryser の定理の最初の証明もそうであったのだが) Hasse-Minkowski の2次形式の有理同値性に関する深い結果が必要とされる．

定理 20.9.10. (**Hughes**). π を位数 n の平面とし，n は Bruck-Ryser 条件を満たすとする．(すなわち，$n\equiv 1, 2 \pmod 4$ で，n は2つの平方数の和として表わされない．) さらに，G を π の共線変換からなる，位数が奇素数 p の群とし，G により固定される点の個数 u が偶数であと仮定する．このとき方程式，

$$x^2=ny^2+(-1)^{(p-1)/2}pz^2$$

は整数解 x, y, z (少なくとも1つは零でない) を持つ．

同じ結果は，位数が奇数 g の共線変換群 G に対しても，G の各元 $\neq 1$ が同じ点達を固定するという条件のもとで成り立つ．

この Hughes の結果は，先の Bruck-Ryser の定理と同じように，ある種の共線変換が存在しないことを示している．ただし，これらの条件が満たされたとしても，共線変換が，実際，存在するとは保証されない．

以下で述べることの主要な点は，もし平面πがある種の共線変換からなる群を持てば，πはさらに，他の特別な共線変持を持たなければならない，ということである．簡単のために，Gはπの $N=n^2+n+1$ 個の点の上に可移で正則であると仮定し，さらにGはアーベル群であると仮定する．この結果は，最初，Hall [3] により，Gが位数Nの巡回群で，N個の点の集合の上に可移である場合に示された．次に，Bruck [1] は，Gが可移で正則ならば，アーベル群という仮定なしに，同じ結果が成り立つことを示した．一方，Hoffman [1] は，Gがπの L_∞ 上になく，原点と異なるような n^2-1 個の点の上に巡回的に働くという仮定のもとに，同じ結論を得た．

さて，位数nの平面πの共線変換の作るアーベル群Gで，πのN個の点の上に可移かつ正則なものが与えられていると仮定する．ここで，Pをπの固定した1点とすれば，各点は Px, $x\in G$ と一意的に表わされる．もし整数tがNと互いに素であれば，$x\to x^t$, $x\in G$ はGの自己同型である．任意の $x\in G$ に対して $Px\to Px^t$ がπの共線変換となるとき，tをπの乗法因子 (multiplier) とよぶことにする．直ちに分かるように，乗法因子の集合は，Nを法として乗法群を作る．

定理 20.9.11. 位数nの平面πが，共線変換の作るアーベル群GでさらにπのN個の点の上に可移かつ正則なものを持つと仮定する．このとき，nを割る任意の素数はπの乗法因子である．

証：仮定により，Gはπの点の集合の上に可移であるから，Gはπの直線の集合の上に可移である．（すなわち $w=1$）それゆえ，1点 $P=P_1$ および1直線 $L=L_1$ をそれぞれの可移域の代表系としてとれる．もし，$D_{11}=\{x_1, x_2, \cdots, x_{n+1}\}$, $x_i\in G$ であれば，Px_i, $i=1,\cdots,n+1$ 達が L_1 の点の集合である．したがって，$Px_1u,\cdots,Px_{n+1}u$, $u\in G$ 達は L_u の点である．ここで $D=\delta_{11}$, $D'=\delta_{11}{}^*$ すなわち

$$D=x_1+\cdots+x_{n+1}$$

$$D'=x_1{}^{-1}+\cdots+x_{n+1}{}^{-1}$$

であり，C_2 と C_1 は単位元である．また，(20.9.25) の最初の2つの関係式は

(20.9.33) $$DD'=D'D=n\cdot 1+\gamma$$

で表わされる．一方，(20.9.25) の後の2つの関係式からは，D および D' は $n+1$ 個の元しか含まないということしか出てこない．さて，$Px\to Px^p$ が π の共線変換になることを示そう．このためには，$Px_1{}^p$, $Px_2{}^p$, $\cdots$, $Px_{n+1}{}^p$ が1直線上にあることを示しさえすればよい．また，このためには，各直線 Lu 上の点の集合は Px_1u, Px_2u, $\cdots$, $Px_{n+1}u$ と表わされるから，G のある元 u が存在して

(20.9.34) $$D^{(p)}=x_1{}^p+\cdots+x_{n+1}{}^p=(x_1+\cdots+x_{n+1})u$$

が成り立つことを示せばよい．逆に，もし (20.9.34) が成り立てば，$Px_1{}^p$, $\cdots$, $Px_{n+1}{}^p$ は L_v の点の集合であり，したがって，$P(x_1v)^p$, $\cdots$, $P(x_{n+1}v)^p$ は Luv^p の点の集合である．したがって，$Px\to Px^p$ は共線変換となり，p は乗法因子となる．さて，ここでは，G^* を G の有理整数環 Z 上の群環とし，G^* (mod p) で係数 p を法として考えた群環を表わす．いま，G はアーベル群であるから，各多項係数は p の倍数であり，したがって，

(20.9.35) $$D^{(p)}=x_1{}^p+\cdots+x_{n+1}{}^p\equiv(x_1+\cdots+x_{n+1})^p=D^p \pmod{p}$$

が成り立つ．仮定より，$p|n$，また $N=n^2+n+1$ であるから $(p, N)=1$ である．また $p|n$ により，(20.9.33) から，

(20.9.36) $$DD'\equiv\gamma \pmod{p}$$

が得られる．D^{p-1} を両辺に乗ずることにより，

(20.9.37) $$D^pD'\equiv D^{p-1}\gamma\equiv(n+1)^{p-1}\gamma\equiv\gamma \pmod{p}$$

が得られる．したがって，(20.9.35) から

(20.9.38) $$D^{(p)}D'\equiv\gamma \pmod{p}$$

である．したがって

(20.9.39) $$D^{(p)}D'=\gamma+pR$$

と表わせる．ここで（このことが，この証明の一番重要な点なのだが）R における群の元の係数は，負でない整数である．なぜならば，$D^{(p)}D'$ において，各係数は負でない整数であり，(20.9.38) により，各項 a_iu_i, $u_i\in G$ の係数に

対して $a_i\equiv 1 \pmod p$, $a_i\geqq 0$ が成り立つからである．したがって $a_i\geqq 1$ であり，$(a_i-1)/p$ は負でない整数であり，これはまた R における u_i の係数を表わす．いま，$x\to x^{-1}$, $x\in G$ は G の自己同型だから，それは $h\in G^*$ に対して自己同型 $h\to h'$ を定める．またこの自己同型により $D\to D'$ である．したがって，この自己同型を（20.9.39）に適用すれば，

(20.9.40) $$DD'^{(p)}=\gamma+pR'$$

が得られる．また，$x\to x^p$ も G の自己同型だから，この自己同型も G^* の自己同型 $h\to h^{(p)}$ を定める．ここで，この自己同型を（20.9.33）に適用すれば，

(20.9.41) $$D^{(p)}D'^{(p)}=n\cdot 1+\gamma$$

が得られる．そこで，（20.9.33）と（20.9.41）の積は，（20.9.39）と（20.9.40）の積と等しいから，

(20.9.42) $$(n\cdot 1+\gamma)^2=(\gamma+pR)(\gamma+pR')$$

が成り立つ．$x\to 1$ $(x\in G)$ で G から Z 有理整数環 Z への準同型を定め，これを（20.9.39）に適用すれば

(20.9.43) $$(n+1)^2=n^2+n+1+pR(1)$$

となる．ここで $R\to R(1)$ は上で定めた準同型写像を表わす．したがって，$pR(1)=n$ であり $pR'(1)=n$ である．一方 G^* においては，$pR\gamma=pR(1)\gamma=n\gamma$ である．（20.9.42）をこれを用いて書き直せば，

(20.9.44) $$n^2\cdot 1=(pR)(pR')$$

を得る．しかし pR および pR' はいずれも係数が負でないから，pR において，0でない係数を持った元はただ一つ，すなわち $pR=bu$, $u\in G$, $b>0$, $b\in Z$ でなければならない．したがって $b=pR(1)=n$ であり，$pR=nu$ である．これを用いて（20.9.39）を書き直せば，

(20.9.45) $$D^{(p)}D'=\gamma+nu$$

が得られる．D を両辺に乗じ（20.9.33）を用いれば，

$$D^{(p)}D'D=\gamma D+nDu$$

(20.9.46) $$D^{(p)}(n+\gamma)=(n+1)\gamma+nDu$$

$$nD^{(p)}+(n+1)\gamma=(n+1)\gamma+nDu$$

が得られる．したがって

(20.9.47) $$D^{(p)}=Du$$

が得られる．したがって (20.9.34) が成り立つから，定理の証明は完成した．証終．

この定理がいかに役立つかを示すために，例として，位数 8 の平面で，位数73の共線変換群（巡回群になる）を持つものを考えよう．mod 73 による剰余類の集合を点の集合とおく．このとき，2 は乗法因子となるから，もし a_1, …, a_9 が 1 直線上の点の集合であれば，$\{2a_1, \cdots, 2a_9\}$ は適当な s に対して $\{a_1+s, \cdots, a_9+s\}$ と等しい．そこで，点 $a_1-s, \cdots, a_9-s$ は乗法因子 2 により固定される 1 直線上にある．もし，それらの剰余類のうちに 1 が含まれれば，乗法因子 2 により，その直線上の点がすべて定まる．すなわち，1, 2, 4, 8, 16, 32, 37, 55, 64 (mod 73) である．乗法因子 2 により固定される任意の直線は，これと定数因子だけ異なり，同じ平面を与える．すなわち，位数 8 の平面で，位数73の共線変換群を持つものは一意的に定まる．したがって，定理 20.9.5 により，デザルグ平面は，そのような共線変換群を持つから，この平面はデザルグ平面でなければならないことが示された．

Hughes はさらに，定理 20.9.10 よりも特殊で，精密な結果を証明した．

定理 20.9.12. $n\equiv 2 \pmod 4$, $n>2$, ならば，位数 n の平面 π は対合 (involution) を持たない．

証：位数 n の平面 $\pi(n\equiv 2 \pmod 4), n>2)$ が対合 b を持つと仮定する．n は偶数で，かつ平方数でないから，定理 20.9.7 により，b は相応である．相応 b の軸を M，中心を $C(\in M)$ とする．M 上の C と異なる点達を Q_i, $i=1, \cdots, n$, C を通り M と異なる直線達を K_i, $i=1, \cdots, n$ で表わす．$n=2m$ と置く，したがって，m は奇数である．点 C を通らないような n^2 個の直線達は，それぞれが 2 つの直線，L と Lb, からなるような $n^2/2=2m^2$ 個の組に分かれる．各組から直線を 1 つづつ選び，それらを L_i, $i=1, \cdots, 2m^2$ とする．一方，同様にして，K_i 上 C と異なる点の全体は，2 つづつ，$n/2=m$ 個の組に分かれ

る．この各組から１つづつ点を選び，それらを，P_{ij}, $j=1, \cdots, (n/2)=m$ とする．次に，インシデンス数 $a_{ij}{}^k$ を次の規則により定める．

(20.9.48)
$$\begin{aligned} a_{ij}{}^k &= +1, \quad P_{ij} \in L_k \text{ のとき} \\ a_{ij}{}^k &= -1, \quad P_{ij}b \in L_k \text{ のとき} \\ a_{ij}{}^k &= 0, \quad \text{その他の場合} \end{aligned}$$

補題 20.9.3. $$\sum_k (a_{ij}{}^k)^2 = n$$

補題 20.9.4. $(i, j) \neq (s, t)$ ならば $\sum_k a_{ij}{}^k a_{st}{}^k = 0 \cdots\cdots\cdots (*)$

補題 20.9.3 の証：点 P_{ij} を通り，Cを通らない直線（すなわち L_k または $L_k b$ という形の直線）は n 個ある．証終．

補題 20.9.4 の証：1）$i=s$, $j \neq t$ と仮定する．点 P_{ij}, P_{it}, $P_{ij}b$, $P_{it}b$ はいづれも直線 K_i 上にある．したがって任意の $k(k=1, \cdots, 2m^2)$ に対して $a_{ij}{}^k a_{it}{}^k = 0$ である．したがって，式（$*$）の左辺の和は零である．2）$i \neq s$ と仮定する．直線 $P_{ij}P_{st} = L_q x$, $P_{ij}P_{st}b = L_r y$（ここで x, y は１または b）とする．もし $r=q$, $x=y$ であれば $L_q x = L_r y$ は K_s 上の相異なる２点 P_{st} と $P_{st}b$ を含み矛盾である．また，$r=q$, $x=yb$ であれば，$L_q x = L_r yb$ は K_i 上の相異なる２点 P_{ij} と $R_{ij}b$ を含み矛盾である．したがって $r \neq q$ である．したがって，

$$a_{ij}{}^q = a_{st}{}^q, \quad a_{ij}{}^q a_{st}{}^q = +1$$
$$a_{ij}{}^r = -a_{st}{}^r, \quad a_{ij}{}^r a_{st}{}^r = -1$$

であるから，式（$*$）の零と異なる項を２つづつくくったものは零，したがって式（$*$）の左辺の和は零である．証終．

上で定義したインシデンス数 $a_{ij}{}^k$ 達を用いて $2m^2 \times 2m^2$ のインシデンス行列

(20.9.49) $$A = (a_{ij}{}^k) \qquad ij \text{ 行，} k \text{ 列．}$$

を定める．上の２つの補題から分かるように，

(20.9.50) $$AA^T = nI$$

が成り立つ．次に数 b_{ik} を次のように定める．

(20.9.51) $$b_{ik}=\sum_{j=1}^{m} a_{ij}{}^{k},\quad i=1,\cdots,n,\quad k=1,\cdots,2m^2.$$

各直線 L_k と K_i は唯一点で交わるから，b_{ik} の値は $+1$ または -1 である．$n\times 2m^2$ 行列 B を

(20.9.52) $$B=(b_{ik}),\quad i=1,\cdots,n,\quad k=1,\cdots,2m^2$$

で定める．言い換えれば，Bは，Bの第1行はAの最初のm行の和，Bの第2行はAの次のm行の和という具合にして作った行列である．(20.9.50) から分かるように，Aの異なる行の間の内積は零である．したがって，Bに関してもこのことは成り立つ．Bの各列に1または -1 を掛けてやっても，Bの行に関する内積は不変である．このようにしてBの第1行がすべて $+1$ から成るようにしてやる．仮定により $n>2$ であるから，Bには3つ以上の行がある．Bの列を入れ換えることにより，初めの3つの行が

(20.9.53) $$\begin{array}{|cc|cc|}
\multicolumn{2}{|c|}{+1,\quad \cdots\cdots \quad ,+1} & \multicolumn{2}{c|}{+1,\quad \cdots\cdots \quad ,+1} \\
\hline
+1,\cdots,+1 & +1,\cdots,+1 & -1,\cdots,-1 & -1,\cdots,-1 \\
\hline
+1,\cdots,+1 & -1,\cdots,-1 & +1,\cdots,+1 & -1,\cdots,-1 \\
\multicolumn{1}{c}{r} & \multicolumn{1}{c}{s} & \multicolumn{1}{c}{t} & \multicolumn{1}{c}{u}
\end{array}$$

という具合にできる．第1行と第2行および第3行の間の内積は零であるから，$r+s=t+u$, $r+t=s+u$ である．また，$r+s+t+u=2m^2$ である．したがって，

(20.9.54) $$r+s=t+u=m^2,\quad r+t=s+u=m^2$$

したがって，$u=r$, $s=t=m^2-r$ である．一方第2行と第3行の間の内積は零であるから，$r+u=s+t=m^2$, したがって，

(20.9.56) $$2r=m^2$$

である．しかし，$n\equiv 2 \pmod 4$, $n=2m$, mは奇数であるから，これは矛盾である．したがって π は対合を持たない．証終．

この結果は(20.9.25)の関係から，適当に番号づけを変えて，G^*を整数の上

へ，$1 \to 1$, $b \to -1$ なる準同型によって写すことによっても得ることができる．

Veblen-Wedderburn [1] は，位数 9 の非デザルグ平面を与えた．これが非デザルグ平面の最初の例であるが，さらに，Hughes [2] は，この位数 9 の非デザルグ平面がその中に現われるような Hughes 平面とよばれている無限個の非デザルグ平面からなる一つの系列を見出した．以下で，この，Hughes 平面を構成する．

Hughes 平面の構成：$q=p^r$，p は奇素数とし，中心 Z が $GF(q)=GF(p^r)$ である位数 q^2 の擬体をKと置く．(このような擬体Kの存在はすでに示した．)

$K\times K\times K$ の次のような部分集合 $P=\{(xk, yk, zk)$；x, y, z は少なくとも1つは零でない，Kの固定された元，$k\in K$，$k\neq 0\}$ を点とよぶことにする．Singer の定理 (20.9.5) により，

(20.9.57)
$$\begin{aligned} x &\longrightarrow a_{11}x+a_{12}y+a_{13}z \\ y &\longrightarrow a_{21}x+a_{22}y+a_{23}z \\ z &\longrightarrow a_{31}x+a_{32}y+a_{33}z \end{aligned}$$

$a_{ij}\in Z$ (Kの中心)，なる写像で，

$$(x, y, z)=P \longrightarrow PA=(a_{11}x\cdots, \cdots, a_{33}z)$$

が，z で座標づけられた位数 q のデザルグ平面の，位数 $m=q^2+q+1$ の共線変換 α となるものが存在する．

次に，$t=1$ または $t\notin Z$ なる t に対して，基底直線 L_t とよばれるものを記号的に定める．したがって，基底直線は，$1+(q^2-q)=q^2-q+1$ 個存在する．そこでインシデンス $P=(xk, yk, zk)\in L_t$ を x, y, z が式

(20.9.59)
$$x+ty+z=0$$

を満たすことで定義すれば，この定義は意味を持つ．なぜならば，K において，乗法の結合律と右分配律が成り立つから (20.9.59) により

(20.9.60)
$$0=(x+ty+z)k=xk+t(yk)+zk$$

が成り立ち，式 (20.9.59) が成り立つか否かは，P の代表元のとり方によらないからである．

次に，記号的に，$L_t\alpha^i$，$i=0, \cdots, m-1$ を直線と定め，さらに点とのイシン

(20.9.65) $$uy+az+t(vy+bz)=0$$

が得られる．ここで

(20.9.66)
$$\begin{aligned} u&=b_{12}+b_{32}-(b_{11}+b_{31})s \\ v&=b_{22}-b_{21}s \\ a&=b_{13}+b_{33}-(b_{11}+b_{31}) \\ b&=b_{23}-b_{21} \end{aligned}$$

である．ここで，$a, b \in Z$ であるが，u, v はZに含まれるとは限らないことに注意しよう．(20.9.65) を解くために，次の3つの場合にわけて考える．

Case 1. $b \neq 0$, a, b^{-1} が中心に含まれることを用いて (20.,9.65) を書き直せば，

(20.9.67) $$(b^{-1}a+t)(vy+bz)+(u-b^{-1}av)y=0$$

が得られる．もし，係数 $b^{-1}a+t$ と $u-b^{-1}av$ が共に零であれば，$t \in Z$, $t=1$ かつ $a+b=0$, $u+v=0$ である．$u+v=0$ から，

(20.9.68) $$b_{12}+b_{22}+b_{32}=(b_{11}+b_{21}+b_{31})s$$

が得られ $s \in Z$ したがって $s=1$ である．一方 $a+b=0$ から，

(20.9.69) $$b_{13}+b_{23}+b_{33}=b_{11}+b_{21}+b_{31}$$

が得られる．これと，$s=1$, $t=1$ から分かるように，(20.9.63) と (20.9.64) とは $GF(q)$ 上のデザルグ平面 π_1 の同一の直線を定める．したがって，行列 A は π_1 上の位数 $m=q^2+q+1$ の共線変換であることから $L_s=L_1$, $L_t\alpha^i=L_1$ でなければならない．しかし，このためには，(20.9.67) の係数が共に0であってはならないから矛盾であり，したがって (20.9.67) のどちらかの係数は0でない．そこで，まず $b^{-1}a+t \neq 0$ の場合を考える．yを任意にとれば，$vy+bz$ は一意的に定まり，また $b \neq 0$ であるから，z も一意定まる．もし，$b^{-1}a+t=0$ であれば，$u-b^{-1}av \neq 0$, したがって $y=0$ で z は任意である．したがって，y と z は右からの定数倍を除いて，一意的に決まったわけであるが，(20.9.64) により，x も y と z により一意的に定まる．したがって (20.9.63) と (20.9.64) を同時に満たす点 (xk, yk, zk) はただ一つ存在する．

デンス

(20.9.61)　$$PA^i \in L_t\alpha^i,\ \ i=0, \cdots, m-1$$

を $P\in L_t$ により定める．さて，(20.9.59) の解は，x, y を両方がともに零でないように，任意にとったとき，z が一意的に定まるから，q^4-1 通り存在する．このうち．q^2-1 個づつが同一の点を定めるから，L_t は，$q^2+1=n+1$ ($q^2=n$ と置く) 個の相異なる点を含む．したがって，各直線 $L_t\alpha^i$ は $n+1$ 個の点を含む．また，全部で $(q^2-q+1)(q^2+q+1)=q^4+q^2+1=n^2+n+1$ 個の直線があり，各直線は $n+1$ 個の点を含む．また，全部で n^2+n+1 個の点が存在する．さて，上で定めた点と直線の集合が，上で定めたインシデンスにより射影平面になることを示したいのであるが，そのためには，任意の相異なる 2 直線が，ただ 1 点を共有することを示しさえすればよい．いま，写像 $P\to AP$ は 1 対 1 で位数 $m=q^2+q+1$ であるから，もし $\{P\}_s$ が基底直線 L_s 上の点の集合であれば，$L_s\alpha^i$ は点の集合 $\{P\}_sA^i$ を含み，$L_t\alpha^i$ は点の集合 $\{P\}_tA^j$ を含む．したがって $L_s\alpha^i$ と $L_t\alpha^j$ がただ 1 点を共有することを示すためには，L_s と $L_t\alpha^{j-i}=L_t\alpha^h$ がただ 1 点を共有することを示せばよい．(ここで α の巾は m を法として考える．)

$P=(x, y, z)$ が $L_t\alpha^h$ の点であれば PA^{-h} は L_t の点であり，また逆も成り立つ．したがって，もし

(20.9.62)　$$(x, y, z)A^{-h} =(b_{11}x+b_{12}y+b_{13}z, b_{21}x+b_{22}y+b_{23}z, b_{31}x+b_{32}y+b_{33}z)$$

であれば，$P=(x, y, z)$ が $L_t\alpha^h$ 上にあるという条件は，

(20.9.63)　$$(b_{11}x+b_{12}y+b_{13}z)+t(b_{21}x+b_{22}y+b_{23}z) +(b_{31}x+b_{32}y+b_{33}z)=0$$

で表わされる．一方，(x, y, z) が L_s 上にあるという条件は，

(20.9.64)　$$x+sy+z=0$$

で表わされる．したがって，(20.9.63) と (20.9.64) を共に満たす解が右からの定数 k 倍を除いて，一意的に定まることを示せばよい．(20.9.64) から x を解いて (20.9.63) に代入して，

Case 2. $b=0$, $a\neq 0$. (20.9.65) を書き直せば,

(20.9.70) $$(u+tv)y+az=0$$

が成り立つ, $a\neq 0$ であるから, (20.9.70) および (20.9.64) を満たす点 (xk, yk, zk) はただ一つ存在する.

Case 3. $b=0, a=0$. このとき,

(20.9.71) $$b_{13}+b_{33}=b_{11}+b_{31}$$
$$b_{23}=b_{21}$$

が成り立ち, 点 $P=(k, 0, -k)$ は (20.9.65) および (20.9.64) を共に満たす. また, (20.9.71) と (20.9.62) から分かるように,

(20.9.72) $$PA^{-h}=(k, 0, -k)A^{-h}=(b_{11}-b_{13})(k, 0, -k)=P$$

が成り立つ. ここで, A^{-h} は正則行列であるから, $b_{11}-b_{13}\neq 0$ である. 一方 A^h は π_1 の点Pを固定するから, $h\equiv 0 \pmod{m}$ であり, $L_t\alpha^h$ は L_t と等しい. したがって, 我々の考えている直線は L_s と $L_t (s\neq t)$ であるが, これら, $x+sy+z=0$ と $x+ty+z=0$ を同時に満たす点は, $P=(k, 0, -k)$ ただ一つである. いずれの場合にも相異なる2直線はただ一点を共有することが示された. したがって, この平面は射影平面である. ここで作った平面を Hughes 平面とよぶ. 以上を定理としてまとめると,

定理 20.9.13. (Hughes). 位数 q^2 ($q=p^r$, p は奇素数) の擬体Kで, その中心Zが $GF(q)$ となるもの, および, (20.9.57) における写像Aで, 位数qのデザルグ平面上で位数 q^2+q+1 の共線変換であるもの, が与えられているとする. このとき, 直線 $L_t a^i$ が点 PA^i を含むということを, (20.9.59) および (20.9.61) で定義することにより, 位数 q^2 の射影平面ができる.

さらに Hughes は, もし擬体Kが $GF(q^2)$ でなければ, π は非デザルグ平面であり, π は Veblen-Wedderburn 平面とはなり得ないことを示した.

文　　　献

Albert, A. A.

[1] *On nonassociative division algebras,* Trans. Amer. Math. Soc. *72* (1952), 296–309.

Baer, R.

[1] *Erweiterung von Gruppen und ihrer Isomorphismen,* Math. Zeit. *38* (1934), 375–416.

[2] *The decomposition of enumerable primary Abelian groups into direct summands,* Quart. J. of Math. *6* (1935), 217–221.

[3] *The decomposition of Abelian groups into direct summands,* Quart. J. of Math. *6* (1935), 222–232.

[4] *Types of elements and the characteristic subgroups of Abelian groups,* Proc. London Math. Soc. *39* (1935), 481–514.

[5] *The subgroup of elements of finite order of an Abelian group,* Ann. of Math. *37* (1936), 766–781.

[6] *Dualism in Abelian groups,* Bull. Amer. Math. Soc. *43* (1937), 121–124.

[7] *Duality and commutativity of groups,* Duke Math. J. *5* (1939), 824–838.

[8] *The significance of the system of subgroups for the structure of a group,* Amer. J. of Math. *61* (1939), 1–44.

[9] *Abelian groups that are direct summands of every containing Abelian group,* Bull. Amer. Math. Soc. *46* (1940), 800–806.

[10] *Homogeneity of projective planes,* Amer. J. of Math. *64* (1942), 137–152.

[11] *Klassification der Gruppenerweiterungen,* J. reine angew. Math. *187* (1949), 75–94.

[12] *Supersoluble groups,* Proc. Amer. Math. Soc. *6* (1955), 16–32.

Bethe, H. A.

[1] *Termaufspaltung in Kristallen,* Ann. der Physik (5) *3* (1929), 133–208.

Birkhoff, Garrett

[1] *Lattice Theory,* Colloquium publications, Amer. Math. Soc., vol. XXV, rev. ed., 1948.

Birkhoff, G., and MacLane, S.

[1] *A Survey of Modern Algebra*, The Macmillan Co., revised edition, 1953.

Bruck, R. H.

[1] *Difference sets in a finite group*. Trans. Amer. Math. Soc. *78* (1955), 464–481.

Bruck, R. H., and Kleinfeld, E.

[1] *The structure of alternative division rings*, Proc. Amer. Math. Soc. *2* (1951), 878–890.

Bruck, R. H., and Ryser, H. J.

[1] *The non-existence of certain finite projective planes*. Can. J. Math. *1* (1949), 88–93.

Burnside, W.

[1] *On an unsettled question in the theory of discontinuous groups*, Quart. J. Pure and Appl. Math. *33* (1902), 230–238.

[2] *Theory of Groups of Finite Order*, Cambridge Univ. Press, 2nd ed., 1911.

Chowla, S., and Ryser, H. J.

[1] *Combinatorial problems*, Can. J. Math. *2* (1950), 93–99.

Eckmann, B.

[1] *Cohomology of groups and transfer*, Ann. of Math. *58* (1953), 481–493.

Eilenberg, S., and MacLane, S.

[1] *Cohomology theory in abstract groups I*, Ann. of Math. *48* (1947), 51–78.

[2] *Cohomology theory in abstract groups II*, Ann. of Math. *48* (1947), 326–341.

Federer, H., and Jonsson, B.

[1] *Some properties of free groups*, Trans. Amer. Math. Soc. *68* (1950), 1–27.

Frobenius, G.

[1] *Über auflösbare Gruppen IV* Berl. Sitz. (1901), 1223–1225.

[2] *Über einen Fundamentalsatz der Gruppentheorie*, Berl. Sitz. (1903), 987–991.

Gaschütz, W.

[1] *Zur Erweiterungstheorie der Endlichen Gruppen*, J. reine angew. Math. *190* (1952), 93–107.

Gleason, A. M.

[1] *Finite Fano planes*, Amer. J. Math. *78* (1956), 797–807.

Grün, O.

[1] *Beiträge zur Gruppentheorie I*, J. reine angew. Math. *174* (1935), 1–14.

Hall, Marshall, Jr.

[1] *Group rings and extensions*, Ann. of Math. *39* (1938), 220–234.

[2] *Projective planes*, Trans. Amer. Math. Soc. *54* (1943), 229–277. Correction, Trans. Amer. Math. Soc. *65* (1949), 473–474.

[3] *Cyclic projective planes*, Duke Math. J. *14* (1947), 1079–1090.

[4] *Coset representation in free groups*, Trans. Amer. Math. Soc. *67* (1949), 421–432.

[5] *Subgroups of finite index in free groups*, Can. J. Math. *1* (1949), 187–190.

[6] *A basis for free Lie rings and higher commutators in free groups*, Proc. Amer. Math. Soc. *1* (1950), 575–581.

[7] *Subgroups of free products*, Pacific J. Math. *3* (1953), 115–120.

[8] *On a theorem of Jordan*, Pacific J. Math. *4* (1954), 219–226.

[9] *Solution of the Burnside problem for exponent 6*, Proc. Nat. Acad. Sci. *43* (1957), 751–753.

Hall, M. Jr., and Rado, T.

[1] *On Schreier systems in free groups*, Trans. Amer. Math. Soc. *64* (1948), 386–408.

Hall, M. Jr., and Ryser, H. J.

[1] *Normal completions of incidence matrices*, Amer. J. Math. *76* (1954), 581–589.

Hall, Philip

[1] *A note on soluble groups*, J. London Math. Soc. *3* (1928), 98–105.

[2] *A contribution to the theory of groups of prime-power order*. Proc. London Math. Soc. *36* (1933), 29–95.

[3] *On a Theorem of Frobenius*, Proc. London Math. Soc. *40* (1936), 468–501.

Hall, P., and Higman, G.

[1] *The p-length of a p-soluble group, and reduction theorems for Burnside's problem*, Proc. London Math. Soc. (3) *7* (1956), 1–42.

Hardy, G. H., and Wright, E. M.

[1] *An Introduction to the Theory of Numbers*, The Clarendon Press, Oxford, 1938.

Higman, Graham

[1] *On finite groups of exponent five*, Proc. Camb. Phil. Soc. *52* (1956), 381–390.

Hirsch, K. A.

[1] *On infinite soluble groups*, Proc. London Math. Soc. (2) *44* (1938), 53–60.

[2] *On infinite soluble groups II*, *Ibid.* *44* (1938), 336-344.

[3] *On infinite soluble groups III*, *Ibid.* *49* (1946), 184-194.

Hoffman, A. J.

[1] *Cyclic affine planes*, Can. J. Math. *4* (1952), 295-301.

Hölder, O.

[1] *Zuruckführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen*, Math. Ann. *34* (1889), 26-56.

Holyoke, T. C.

[1] *On the structure of multiply transitive permutation groups*, Amer. J. Math. *74* (1952), 787-796.

Hughes, D. R.

[1] *Regular collineation groups*, Proc. Amer. Math. Soc. *8* (1957), 159-164.

[2] *A class of non-Desarguesian projective planes*, Can. J. Math. *9* (1957), 378-388.

[3] *Generalized incidence matrices over group algebras*, Ill. J. Math. *1* (1957), 545-551.

[4] *Collineations and generalized incidence matrices*, Trans. Amer. Math. Soc. *86* (1957), 284-296.

Huppert, B.

[1] *Normalteiler und maximale Untergruppen endlicher Gruppen*, Math. Zeit. *60* (1954), 409-434.

Iwasawa, K.

[1] *Über die endlichen Gruppen und die Verbände ihrer Untergruppen*, J. Univ. Tokyo *43* (1941), 171-199.

Jordan, C.

[1] *Commentaire sur Galois*, Math. Ann. *1* (1869), 141-160.

[2] *Recherches sur les substitutions*, J. Math. Pures Appl. (2) *17* (1872), 351-363.

Kaplansky, I.

[1] *Infinite Abelian Groups*, University of Michigan Press, 1954.

Kleinfeld, E.

[1] *Alternative division rings of characteristic 2*, Proc. Nat. Acad. Sci. USA *37* (1951), 818-820.

[2] *Right alternative rings*, Proc. Amer. Math. Soc. *4* (1953), 939-944.

Kostrikin, A. I.

[1] *Solution of the restricted Burnside problem for exponent 5*, Izv. Akad.

Nauk SSSR, Ser. mat. *19* (1955), 233-244. (In Russian.)

Krull, W.

[1] *Über verallgemeinerte endliche Abelsche Gruppen*, Math. Zeit. *23* (1925), 161-196.

[2] *Theorie und Anwendung der verallgemeinerten Abelschen Gruppen*, Sitz Heidelberg. Akad. Wiss. (*1926*), *1*-32.

Kurosch, A.

[1] *Die Untergruppen der freien Produkte von beliebigen Gruppen*, Math. Ann. *109* (1934), 647-660.

[2] *The Theory of Groups*, 2nd. ed., translated from the Russian by K. A. Hirsch, two volumes, Chelsea Publishing Co., New York, 1955.

Levi, F. W.

[1] *Über die Untergruppen der freien Gruppen*, Math. Zeit. *32* (1930), 315-318.

Levi, F. W., and van der Waerden, B. L.

[1] *Über eine besondere Klasse von Gruppen*, Abh. Math. Sem. Hamburg *9* (1933), 154-158.

MacLane, S.

[1] *A conjecture of Ore on chains in partially ordered sets*, Bull. Amer. Math. Soc. *49* (1943), 567-568.

[2] *Cohomology theory in abstract groups, III*, Ann. of Math. *50* (1949), 736-761.

Magnus, W.

[1] *Über Beziehungen zwischen höheren Kommutatoren*, J. reine angew. Math. *177* (1937), 105-115.

[2] *On a theorem of Marshall Hall*, Ann. of Math. *40* (1939), 764-768.

[3] *A connection between the Baker-Hausdorff formula and a problem of Burnside*, Ann. of Math. *52* (1950), 111-126.

Mann, H. B.

[1] *On certain systems which are almost groups*, Bull. Amer. Math. Soc. *50* (1944), 879-881.

Meier-Wunderli, H.

[1] *Note on a basis for higher commutators*, Commentarii Math. Helvetici, *16* (1951), 1-5.

Miller, G. A.

[1] *Limits of the degree of transitivity of substitution groups*, Bull. Amer. Math. Soc., *22* (1915), 68-71.

Moufang, R.

[1] *Alternativkörper und der Satz vom vollständigen Vierseit*, Abh. Math. Sem. Hamburg, *9* (1933), 207-222.

Neumann, B. H.

[1] *Die Automorphismengruppe der freien Gruppen*, Math. Ann. *107* (1932), 367-386.

[2] *On the number of generators of a free product*, J. London Math. Soc. *18* (1943), 12-20.

Neumann, H.

[1] *Generalized free products with amalgamated subgroups I*, Amer. J. Math. *70* (1948), 590-625.

[2] *Generalized free products with amalgamated subgroups II*, *Ibid.* *71* (1949), 491-540.

Nielsen, J.

[1] *Om Regnig med ikke-kommutative Faktorer og dens Anvendelsei Gruppeteorien*, Mat. Tidsskrift B (1921), 77-94.

Noether, E.

[1] *Hyperkomplexe Zahlen und Darstellungstheorie*, Math. Zeit. *30* (1929), 641-692.

Ore, O.

[1] *Direct Decompositions*, Duke Math. J. *2* (1936), 581-596.

[2] *On the theorem of Jordan-Hölder*, Trans. Amer. Math. Soc. *41* (1937), 266-275.

[3] *Chains in partially ordered sets*, Bull. Amer. Math. Soc. *49* (1943), 558-566.

Ostrom, T. G.

[1] *Double transitivity in finite planes*, Can. J. Math. *8* (1956), 563-567.

Parker, E. T.

[1] *On collineations of symmetric designs*, Proc. Amer. Math. Soc. *8* (1957), 350-351.

Pauli, W.

[1] *Zur Quantenmechanik des Magnetischen Elektrons*, Zeit. für Physik, *43* (1927), 601-623.

Pickert, G.

[1] *Projektive Ebenen*, Springer (1955).

Pontrjagin, L.

[1] *Topological Groups*, translated from the Russian by Emma Lehmer, Princeton University Press, 1939.

Prüfer, H.

[1] *Theorie der abelschen Gruppen I*, Math. Zeit. *20* (1924), 165-187.

[2] *Theorie der abelschen Gruppen II*, Math. Zeit. *22* (1925), 222-249.

Remak, R.

[1] *Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren*, J. reine angew. Math. *139* (1911), 293-308.

[2] *Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren*, J. reine angew. Math. *153* (1923), 131-140.

Sanov, I. N.

[1] *Solution of Burnside's problem for exponent 4*, Leningrad State Univ. Ann. *10* (1940), 166-170. (In Russian.)

San Soucie, R. L.

[1] *Right alternative division rings of characteristic two*, Proc. Amer. Math. Soc. *6* (1955), 291-296.

Schmidt, O.

[1] *Über die Zerlegung endlicher Gruppen in direkte unzerlegbare Faktoren*, Izvestiya Kiev Univ. (1912), 1-6.

Schreier, O.

[1] *Über die Erweiterung von Gruppen, I*, Monats. für Math. u. Phys. *34* (1926), 165-180.

[2] *Über die Erweiterung von Gruppen II*, Abh. Math. Sem. Hamburg, *4* (1926), 321-346.

[3] *Die Untergruppen der freien Gruppen*, Abh. Math. Sem. Hamburg, *5* (1927), 161-183.

[4] *Über den Jordan-Hölderschen Satz*, Abh. Math. Sem. Hamburg, *6* (1928), 300-302.

Singer, J.

[1] *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. *43* (1938), 377-385.

Skornyakov, L. A.

[1] *Alternative fields*, Ukrain. Mat. Zur. *2* (1950), 70-85. (In Russian.)

[2] *Right alternative fields*, Izv. Akad. Nauk SSSR, Ser, Mat. *15* (1951), 177-184. (In Russian.)

Suzuki, M.

[1] *Structure of a group and the structure of its lattice of subgroups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 10 (1956), Springer, Berlin.

Tarry, G.

[1] *Le problème des 36 officiers*, C. R. Assoc. Fr. Av. Sci. (1900), 122-123; and (1901), 170-203.

Ulm, H.

[1] *Zur Theorie der abzählbar unendlichen abelschen Gruppen*, Math. Ann. *107* (1933), 774-803.

van der Waerden, B. L.

[1] *Moderne Algebra*, 2nd ed., Berlin, 1940.

Veblen, O., and Wedderburn, J. H. M.

[1] *Non-Desarguesian and non-Pascalian geometries*. Trans. Amer. Math. Soc. *8* (1907), 379-388.

Veblen, O., and Young, J. W.

[1] *Projective Geometry*, vol. 1, Ginn and Co., 1910.

Wedderburn, J. H. M.

[1] *On the direct product in the theory of finite groups*, Ann. of Math. *10* (1909), 173-176.

Wielandt, H.

[1] *Abschatzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad*, Schriften des Math. Sem. und des Inst. für angew. Math. der Univ. Berlin, *2* (1934), 151-174.

[2] *Eine Verallgemeinerung der invarianten Untergruppen*, Math. Zeit. *45* (1939), 209-244.

[3] *p-Sylowgruppen und p-Faktorgruppen*, J. reine angew. Math. *182* (1940), 180-193.

Witt, E.

[1] *Über die Kommutativität endlicher Schiefkörper*, Abh. Math. Sem. Hamburg, *8* (1931), 413.

[2] *Treue Darstellung Liescher Ringe*, J. reine angew. Math. *177* (1937), 152-160.

Zassenhaus, H.

[1] *Zum Satz von Jordan-Hölder-Schreier*, Abh. Math. Sem. Hamburg *10* (1934), 106-108.

[2] *Über endliche Fastkörper*, Abh. Math. Sem. Hamburg, *11* (1936), 187-220.

Zorn, M.

[1] *Theorie der alternativen Ringe*, Abh. Math. Sem. Hamburg, *8* (1931), 123-147.

索　　引

【ローマン数字は上巻，イタリック数字は下巻】

記　号　表

記号は標準的なものを使う．集合の包含関係の記号：$A \supseteq B$, A は B を含む，$A \supset B$, A は B を真に含む，$A \subseteq B$, A は B に含まれる，$A \subset B$, A は B に真に含まれる；$a \in A$, a は集合 A に属する；$a|b$, a は b を割り切る，$a \equiv b \pmod{m}$, a は m を法として b と合同．一般的な用法として記号の上に線を引いたものはその記号の否定を表わす．したがって，$p \nmid s$, p は s を割り切らない，$y \notin G$, y は G に属さない．

（ローマン数字は上巻に，イタリック数字は下巻に含まれることを示す）

記　号　表

$f \sim g$，f は g と同値，101

$\Phi(f)=g_i$，g_i は f の剰余類の代表元，107

$a > b$，a は b の直後の元，130

$A_i \triangleleft A_{i-1}$，$A_i$ は A_{i-1} のなかで正規，139

$(x, y)=x^{-1}y^{-1}xy$，交換子，154

$(x_1, \cdots, x_{n-1}, x_n)$，単純交換子，154

$\Phi=\Phi(G)$，G の Frattini 部分群，175

$\mu(m)$，Möbius 関数，*190*

r_+，有理数のつくる加法群，*219*

R_+，実数のつくる加法群，*219*

$Z(p^\infty)$，ある可換群，*220*

$\chi(a)$，指標，*220, 281*

$V_{G\to K}(g)$ または $V(g)$，元 g の移送，*229*

(u, v)，因子団の因子，*248*

$\bar{x}$，剰余類の代表元，*257*

$\oplus$，右イデアルの直和，*288*

$\boxplus$，両側イデアルの直和，*292*

(f_1, f_2)，対称双線形スカラー積，*304*

$\overset{*}{\Pi}$，自由積，*348*

$[x, y]$，Lie 積，*367*

$Q \overset{P}{\to} R$，配影共線変換，*392*

$x \cdot m \circ b$，三項演算，*400*

(x, y, z)，結合子，*427*

群　論（下）　1970©

1970年9月15日　第1刷発行
1976年3月25日　第2刷発行

訳者　榎本彦衛
　　　坂内英一

発行者　吉岡清

京都市左京区田中門前町87
発行所　株式会社　吉岡書店
電話(075)781−4747／振替京都4624

組版／同朋舎・印刷／一進印刷・製本／池田製本

「数学叢書」刊行に際して

最近10数年の数学の進歩はまことにめざましいものがある。発表される数学の重要論文の数は年とともに増し，新しい理論や，新しい概念が応接にいとまがないほど，たえず創造されている。数学の他の諸科学との関係もますます広く，深く，いわゆる数理科学としての発達も著しいものがある。

これらの新しい理論，概念を整理して簡明な解説を与えた世界的名著は，将来数学でなすところあらんと心掛ける若い学徒にとってまことに貴重なものである。若い学生，大学院学生は，これらの名著によって，早く現代数学の概観を得ることができるであろう。新しい数学を研究し秀れた理論を創造するには，著書や論文を読むだけではもちろん十分ではない。しかし“論文を書く”にしても，最小限の基本知識は身につけ，現代数学の概観を察し得る域には達していなければなるまい。

この叢書刊行の企図するところは，数学の各分野にわたり，重要な理論を整理し，簡明な解説を与えた世界的名著を選んで邦訳し，わが国の若い学徒が日本語により，早く高い見地に到達できるようにすることである。また今日の数学，数理科学はきわめて多方面に分化発展しているので，ある分科の専門家が他の分科の最近の発展を知ることは，必ずしも容易でない。専門外の分野にまで知識を拡げようとする際も，名著の訳註解説書が役立つことであろう。

以上の意図のもとにこの「数学叢書」を編んで世に送る次第である。

この叢書に収めるのは，いずれもそれぞれの分野の世界的権威者による定評ある名著である。特に，多くの予備知識を要せず，しかも続いて数学の創造活動に直結させるが如き名著を選んだのである。翻訳はそれぞれその方面の専門家である訳者に依嘱し，各訳書には，さらにわが国の事情を考慮した適切な訳註を加えていただくことにしたのである。

この叢書が若い学徒のよき伴侶となり，研究者によってよく味読され，将来の日本の数学の活発な活動，水準の向上に資するようになることを念願する次第である。（1968年）

編　集・彌永昌吉／岩堀長慶／河田敬義
小松醇郎／福原満洲雄／古屋茂／吉田耕作

第1～3期

フォーサイス・ワソー　藤野精一訳
第1・5巻　偏微分方程式の差分法による近似解法 上下
上 306頁　下 258頁

ケリー　児玉之宏訳
第2巻　位相空間論
324頁

アグモン　村松寿延訳
第3巻　楕円型境界値問題
318頁

ビリングスレイ　渡辺　毅・十時東生訳
第4巻　確率論とエントロピー
——エルゴード理論と情報量——
286頁

コディントン・レヴィンソン　吉田節三訳
第6・11巻　常微分方程式論 上下
上 366頁　下 332頁

ハラナイ　加藤順二訳
第7・9巻　微分方程式 上下
——安定性，振動論，遅れ時間を持った系——
上 354頁　下 298頁

	ミルナー　志賀浩二訳	
第 8 巻	モース理論 ――多様体上の解析学とトポロジーとの関連――	210頁
	ホール　金沢・八牧・榎本・坂内訳	
第10・13巻	群論 上下	上 198頁　下 318頁
	ヒルツェブルフ　竹内勝訳	
第 12 巻	代数幾何における位相的方法	334頁
	ボレビッチ・シャハレビッチ　佐々木義雄訳	
第14・19巻	整数論 上下	上 324頁　下 284頁
	ホール　岩堀信子訳	
第 15 巻	組合せ理論	396頁
	クレイン　牛島照夫・辻岡邦夫訳	
第 16 巻	バナッハ空間における線形微分方程式	482頁
	ホッホシルト　橋本浩治訳	
第 17 巻	リー群の構造	264頁
	パラモドフ　内山・金子・森本訳	
第18・21巻	定数係数線形微分作用素 上下	上 290頁　下 278頁
	アーノルド・アベズ　吉田耕作訳	
第 20 巻	古典力学のエルゴード問題	296頁
	トレーブ　松浦重武訳	
第22・25巻	位相ベクトル空間・超関数・核 上下	上 344頁　下 400頁
	リィー・マーカス　占部・古川・伊藤訳	
第 23 巻	現代の最適制御理論 上下	上 332頁　下 続刊
	スターンバーグ　高橋恒郎訳	
第 24 巻	微分幾何学	426頁

「物理学叢書」刊行に際して

二十世紀の物理学の進歩は，物質の極微の構造の暴露に，物質の精妙な機構の解明に，驚異的な発展，飛躍をもたらした．その結果，新しい自然力の解放，支配を実現化したばかりでなく，新しい物質の創造，生命の謎への挑戦をも企図せしめつつある．更に，既知の自然力の未曽有の強力な駆使さえ可能にしつつある．二十世紀後半に至って，原子力に，あるいはオートメーションに今や第二の産業革命を喚起せんとするに至った原動力は，物理学の開拓的な創造性によることは言をまたない．更に，現在の物理学は，かっての相対論，量子論の出現にも比すべき革命の前夜にあるといわれている．この時に当たり，物理学の新領域の単なる解説，あるいは時局的な技術書ではなく，真にわが国物理学の発展の糧となるべき良書の出版は緊急の必要事といわねばならぬ．ここに「物理学叢書」を編んで世に送る所以である．

この叢書に収められる原著は，いずれもそれぞれの分野の世界的権威者による定評ある名著に限られるが，前述の精神に鑑みその性格，スタイルに特徴あるものを選ぶと共に，その本質において創造的価値高きものを目標とした．

この叢書が，物理学またはその関連分野へ進む学徒に，よき伴侶として用いられ，真にその血肉となり得ることがわれわれの念願であり，更にこの叢書によって伝えられる海外の学風が，広くわが国の教育，研究へのよき刺戟となり，わが国の明日の科学を築く基礎に貢献するところがあれば幸いである．

(1954年12月)

物　理　学　叢　書

編集・小谷正雄／小林　稔／井上　健／山本常信／高木修二

第1期

第1巻	フェルミ　原子核物理学	小林　稔他訳	404頁
第2・9巻	シッフ　新版 量子力学 上下	井上　健訳	上 374頁　下 320頁
第3巻	ガーネイ　統計力学序論	山本常信訳	316頁
第4・8巻	ショックレイ　半導体物理学 上下	川村　肇訳	上 398頁　下 248頁
第5・7巻	ハイトラー　輻射の量子論 上下	沢田克郎訳	上 304頁　下 242頁
第6巻	パイエルス　固体の量子論	碓井恒丸他訳	286頁

ヴァン・ブレック小谷正雄・神戸謙次郎訳
第 10 巻　物質の電気分極と磁性
440頁

第 2 期

ゴールドスタイン　野間 進・瀬川富士訳
第 11 巻　古　典　力　学
504頁

バチェラー　巽 友正訳
第 12 巻　乱　流　理　論
226頁

オッペンハイマー　小林 稔訳
第 13 巻　電　気　力　学
222頁

ランダウ・スモロディンスキー高木修二訳
第 14 巻　原　子　核　理　論
202頁

リープマン・ロシュコ　玉田 珖訳
第 15 巻　気　体　力　学
510頁

フレーリッヒ　永宮健夫・中井祥夫訳
第 16 巻　誘　電　体　論
234頁

モット・マッセイ　高柳和夫他訳
第 18 巻　新版 衝　突　の　理　論
（全4巻）上・Ⅰ292頁／上・Ⅱ328頁他続刊

パノフスキー・フイリップス林忠四郎他訳
第19・20巻　新版 電　磁　気　学 上下
上 288頁　下 290頁

第 3 期

ドーデル他　大鹿 譲他訳
第21・22巻　量　子　化　学
570頁

アイリング他　平井西夫他訳
第23・24巻　絶 対 反 応 速 度 論 上下
上 328頁　下 350頁

アブラガム　富田和久・田中基之訳
第25・27巻　核　の　磁　性 上下
上 336頁　下 410頁